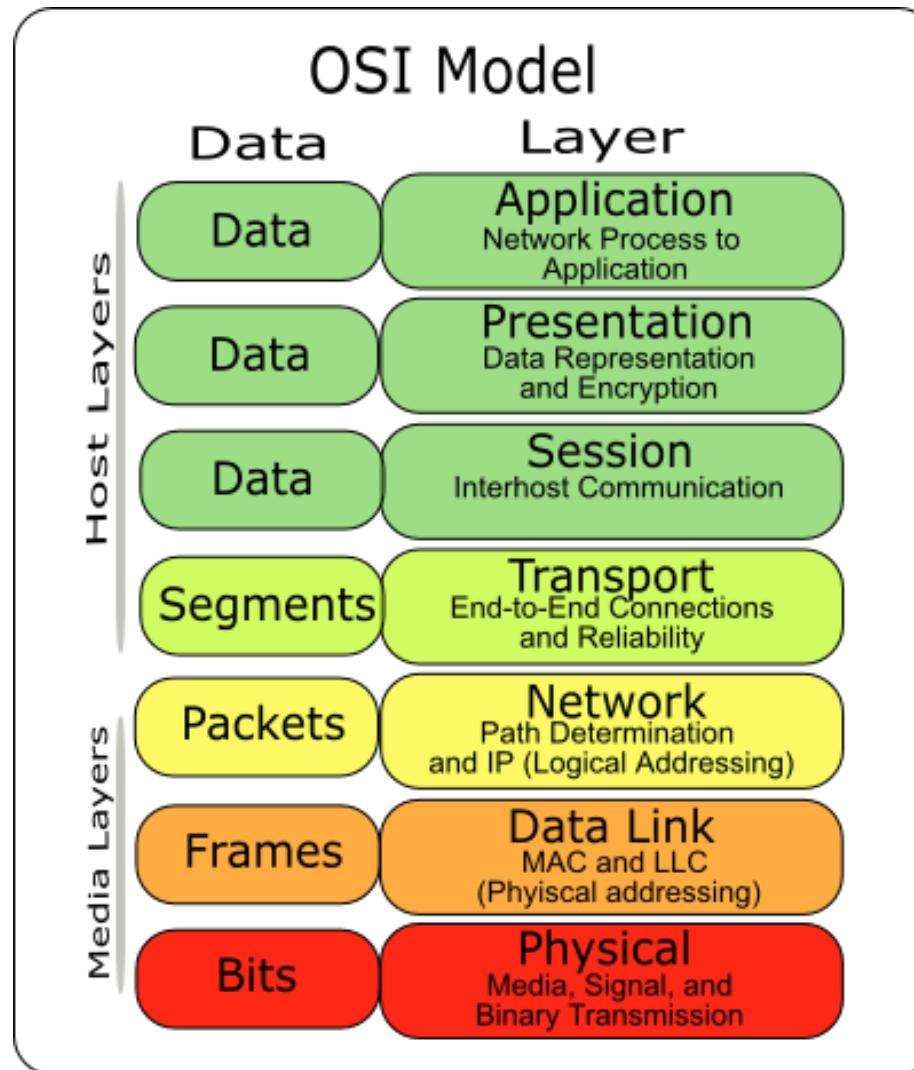


CAPA DE RED

COMUNICACIÓN DE HOST A HOST



TAREAS A REALIZAR

Direccionamiento de paquetes con una dirección IP.

Encapsulamiento.

Enrutamiento.

Desencapsulamiento.

PROTOCOLOS

Comunes

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

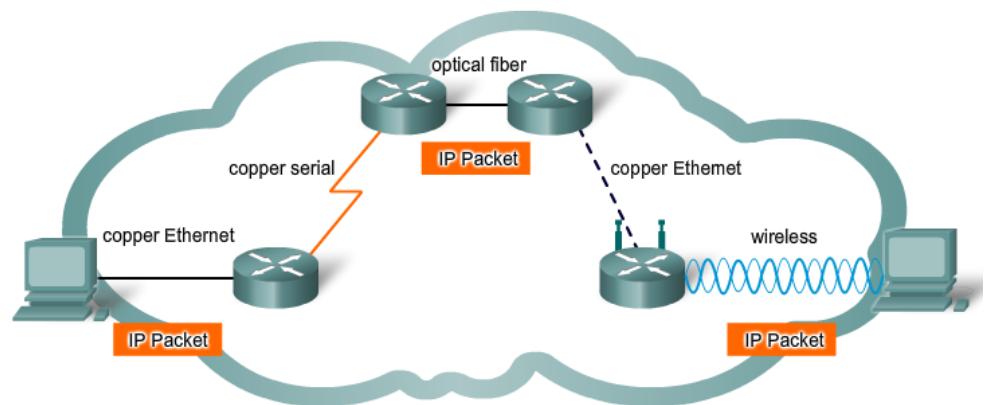
Legado

- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

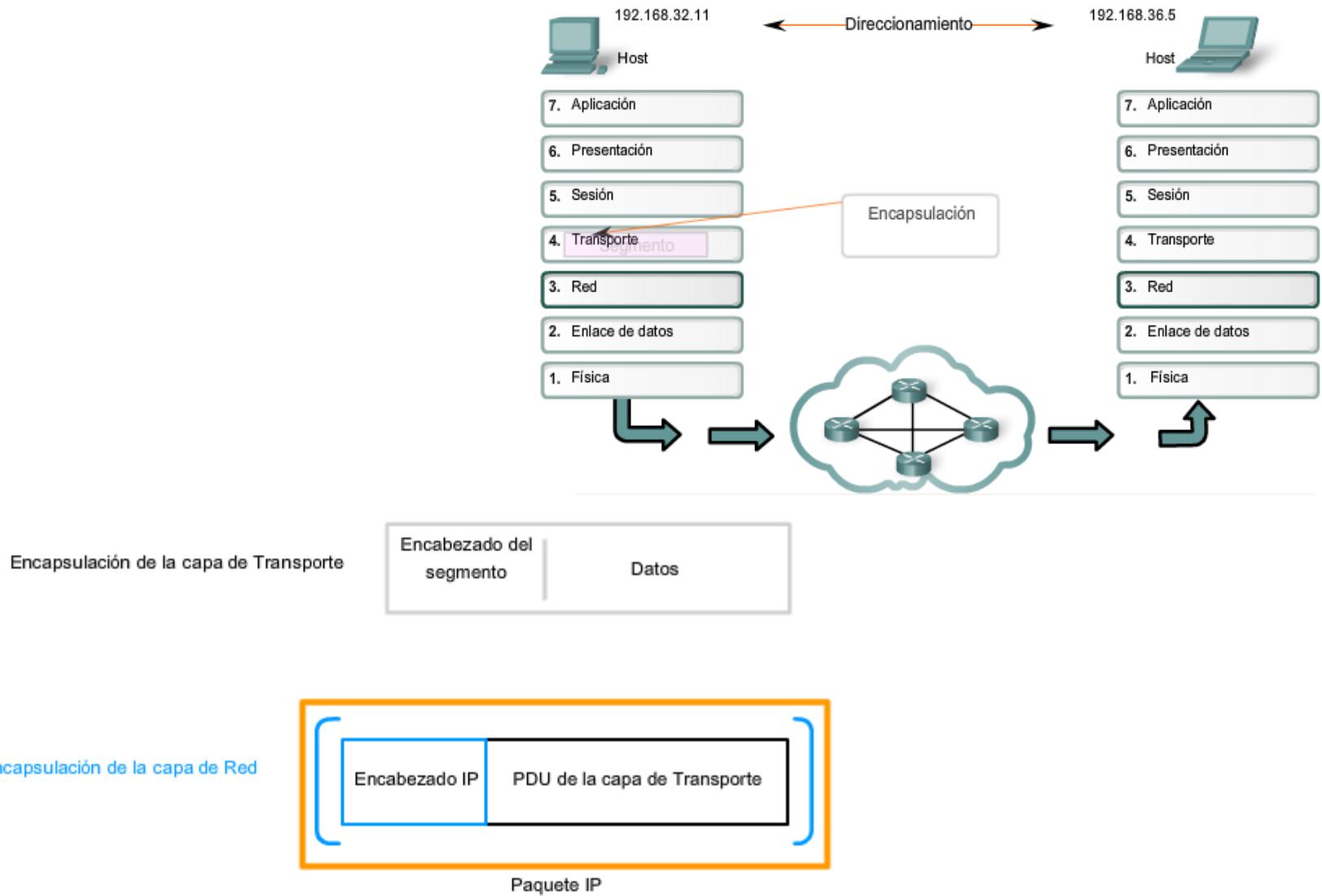
CARACTERÍSTICAS IP



- ❖ Conexión orientada a la no conexión
- ❖ “Mejor Esfuerzo”, no garantiza la entrega de los paquetes
- ❖ Independiente del Medio



ENCAPSULAMIENTO



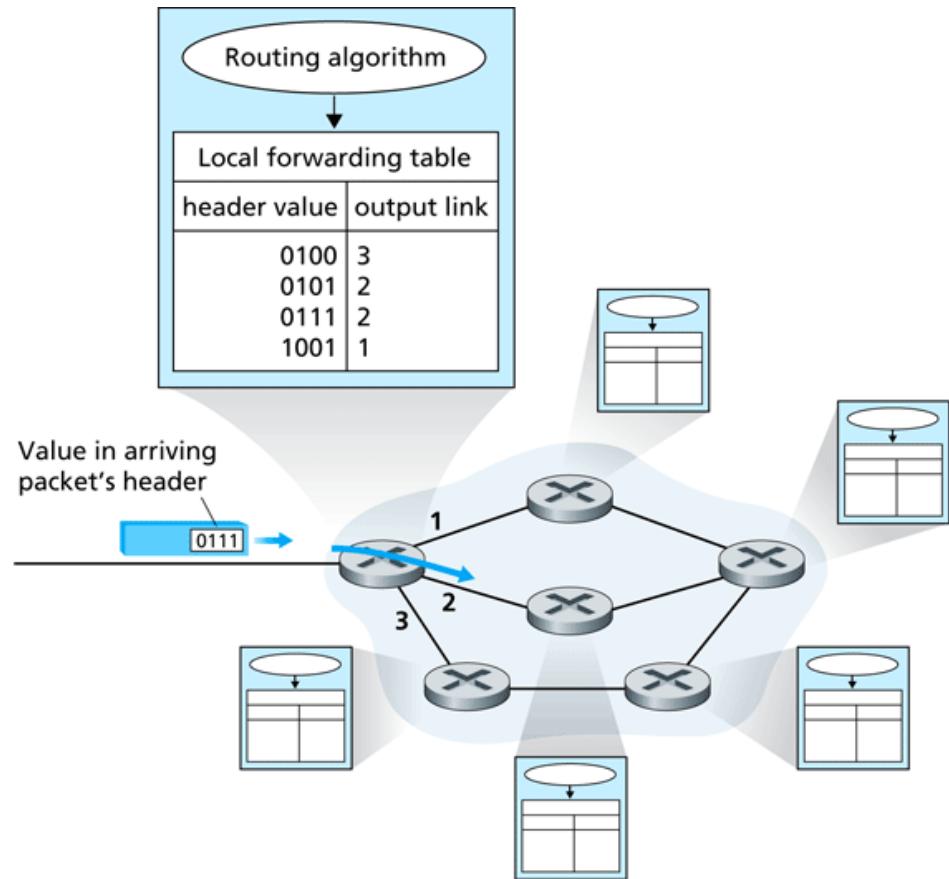
ENRUTAMIENTO

Enrutadores

Proceso de enrutamiento

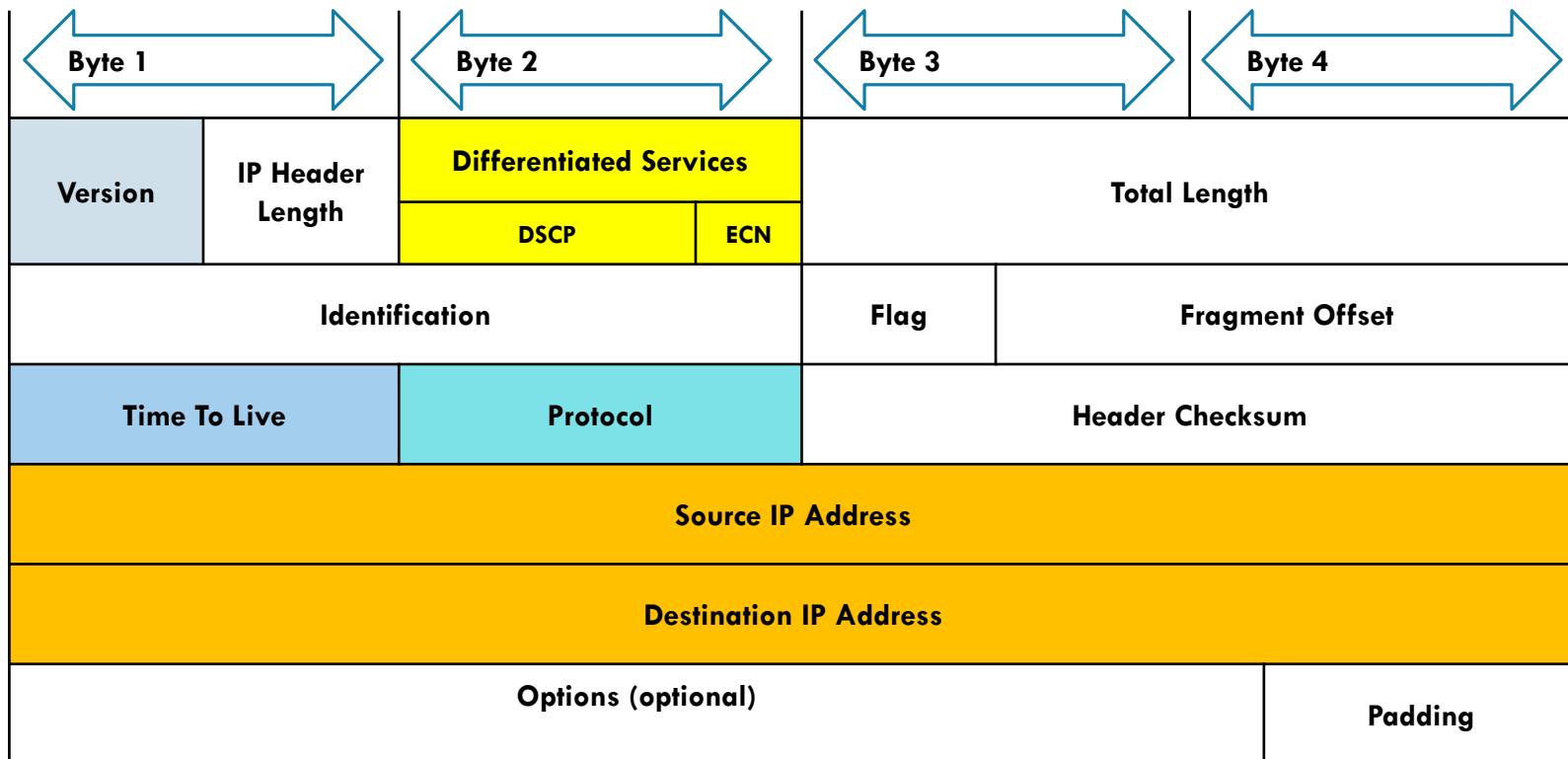
Salto

Red directamente conectada



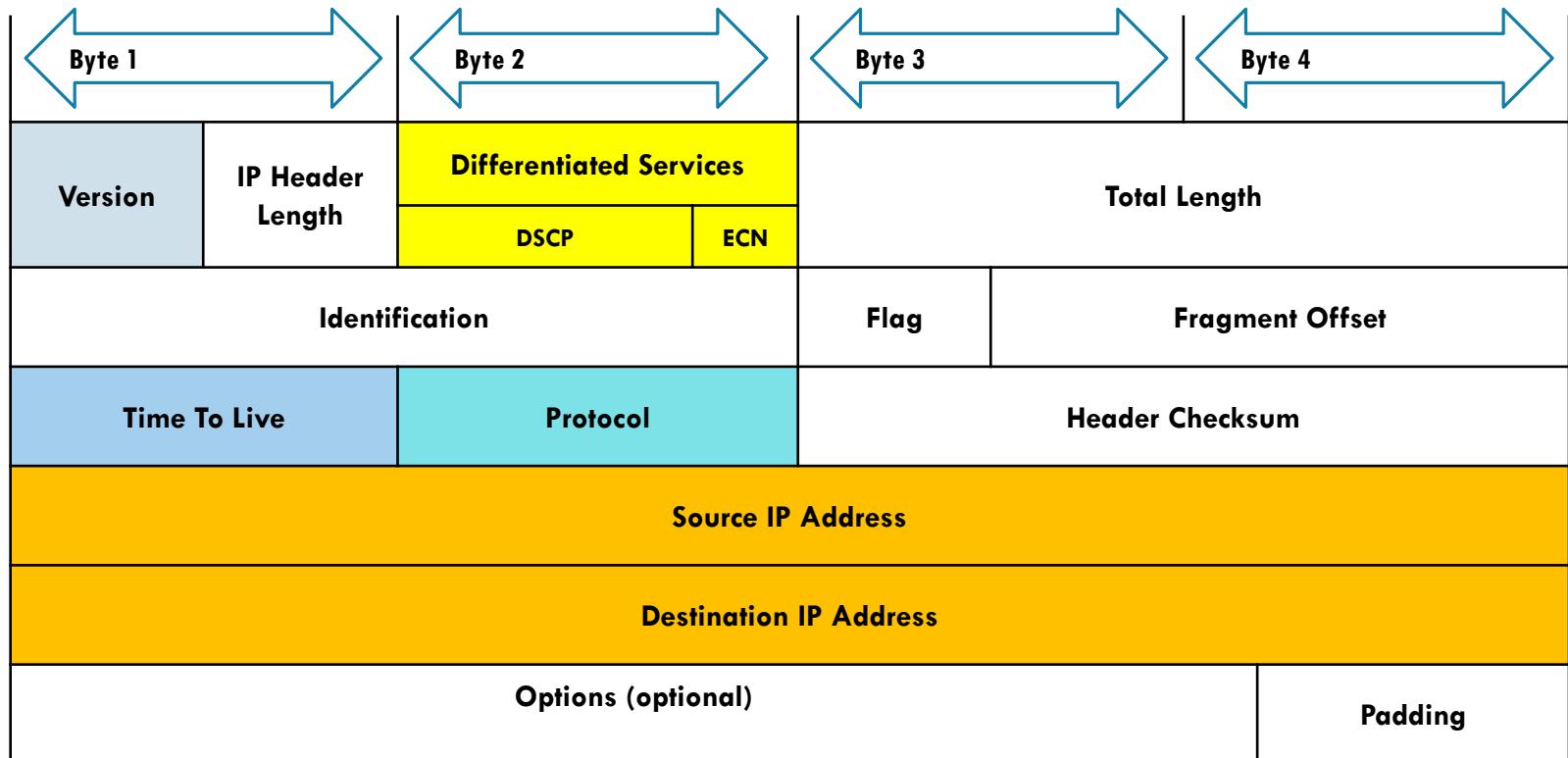
PAQUETE IPV4

Version, Differentiated Services (DS), Time-to-Live (TTL), Protocol, Source IP Address, Destination IP Address



CAMPOS IPV4

Internet Header Length (IHL), Total Length, Header Checksum, Identification, Flags, Fragment Offset



EJEMPLO PAQUETE IPV4

Microsoft: \Device\NPF_{7B83C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 Win=16661 Len=0
19	4.19945400	fe80::15ff:98d8:d28ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28fe80::blee:c4ae:a11		SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP-	154	DroboX LAN svnc Discovery Protocol

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 60
Identification: 0x3704 (14084)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0x7ffe [correct]
Source: 192.168.1.109 (192.168.1.109)
Destination: 192.168.1.1 (192.168.1.1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

Internet Control Message Protocol

0000 00 18 39 a0 d1 be 24 77 03 45 5d c4 08 00 45 00 \$w . E] . . . E.
0010 00 3c 37 04 00 00 80 01 7f fe c0 a8 01 6d c0 a8	. . <7 m . .
0020 01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66 M V . . . abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69	wabcfedg hi

Internet Protocol Version 4 (ip), 20 bytes

Packets: 35 Displayed: 35 Marked: 0 Dropped: 0

Profile: Default

LIMITACIONES DE IPV4

- ✓ El agotamiento de direcciones IP
- ✓ Expansión de la tabla de enrutamiento
- ✓ Falta de conectividad de extremo a extremo



INTRODUCCIÓN A IPV6

- ✓ El aumento de espacio de direcciones
 - ✓ Mejora el manejo de paquetes
 - ✓ Elimina la necesidad de NAT
 - ✓ La seguridad integrada

4 billones de direcciones IPv4

4,000,000,000

340 decíllones de direcciones IPv6

340,000,000,000,000,000,000,000,000,000,000,000,000,000,000

PAQUETE IPV6

IPv4 and IPv6 Headers

IPv4 Header

Version	IHL	Type of Service	Total Length			
Identification		Flags		Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source Address						
Destination Address						
Options		Padding				

IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length		Next Header	Hop Limit	
Source Address				
Destination Address				

Legend

- Field names kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name & position changed in IPv6
- New field in IPv6

EJEMPLO PAQUETE IPV6

The screenshot shows a Wireshark capture window titled "v6-http.cap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]". The packet list pane displays several TCP segments, with the 49th packet selected. The details pane shows the following information for the selected packet:

- Frame 49: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
- Ethernet II, Src: HsingTec_e3:e8:de (00:d0:09:e3:e8:de), Dst: Ibm_82:95:b5 (00:11:25:82:95:b5)
- Internet Protocol Version 6, src: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de), dst: 2001:6f8:102d:0:2d0:9ff:fee3:e8de
- Version: 6
- Traffic class: 0x00000000
- Flowlabel: 0x00000000
- Payload length: 260
- Next header: TCP (6)
- Hop limit: 64
- Source: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)
[Source SA MAC: HsingTec_e3:e8:de (00:d0:09:e3:e8:de)]
- destination: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 59201 (59201), Dst Port: http (80), Seq: 1, Ack: 1, Len: 240
- Hypertext Transfer Protocol

The bytes pane at the bottom shows the raw hex and ASCII data for the selected IPv6 packet.

TABLA DE ENRUTAMIENTO DE UN HOST

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\L00638650>route print
=====
ILista de interfaces
 13...a4 4e 31 24 52 70 .....Intel(R) Centrino(R) Advanced-N 6205
 12...f0 92 1c 5b 8e 70 .....Intel(R) 82579LM Gigabit Network Connection
   1.....Software Loopback Interface 1
 17...00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft
 10...00 00 00 00 00 00 e0 Adaptador de tunelización Teredo de Microsoft
=====

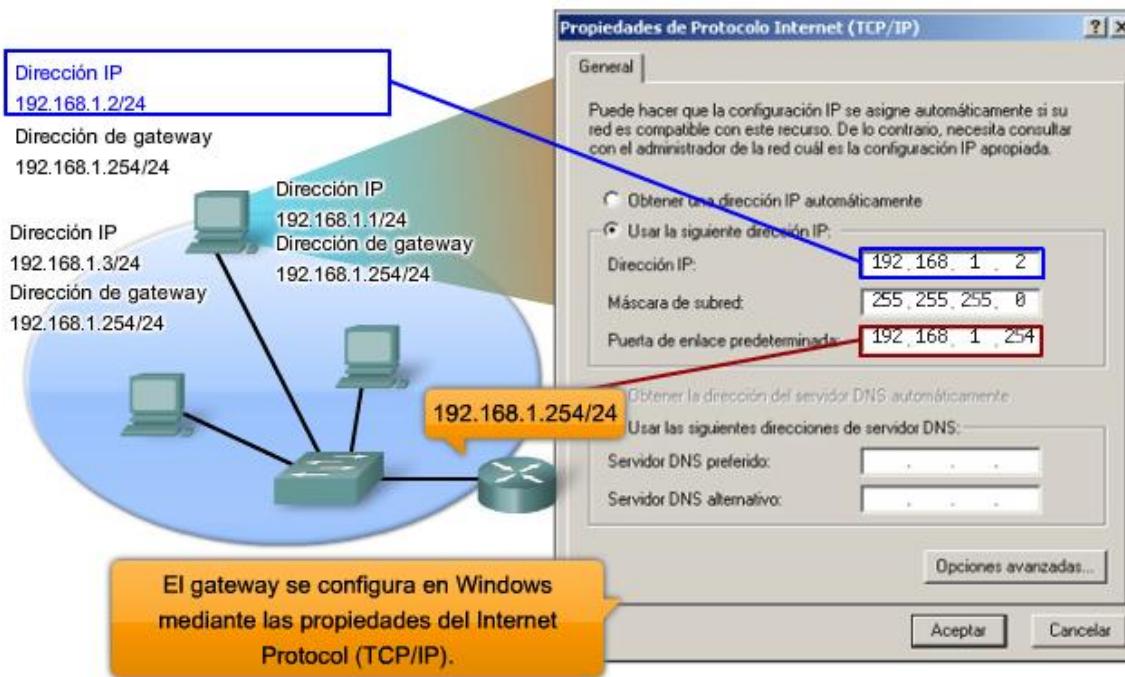
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red    Puerta de enlace  Interfaz   Métrica
          0.0.0.0        0.0.0.0    10.48.82.250  10.48.82.186  25
          10.48.82.0     255.255.255.0  En vínculo       10.48.82.186  281
          10.48.82.186  255.255.255.255 En vínculo       10.48.82.186  281
          10.48.82.255  255.255.255.255 En vínculo       10.48.82.186  281
          127.0.0.0       255.0.0.0    En vínculo       127.0.0.1    306
          127.0.0.1       255.255.255.255 En vínculo       127.0.0.1    306
          127.255.255.255 255.255.255.255 En vínculo       127.0.0.1    306
          224.0.0.0        240.0.0.0    En vínculo       127.0.0.1    306
          224.0.0.0        240.0.0.0    En vínculo       10.48.82.186  281
          255.255.255.255 255.255.255.255 En vínculo       127.0.0.1    306
          255.255.255.255 255.255.255.255 En vínculo       10.48.82.186  281
=====
Rutas persistentes:
 Ninguno

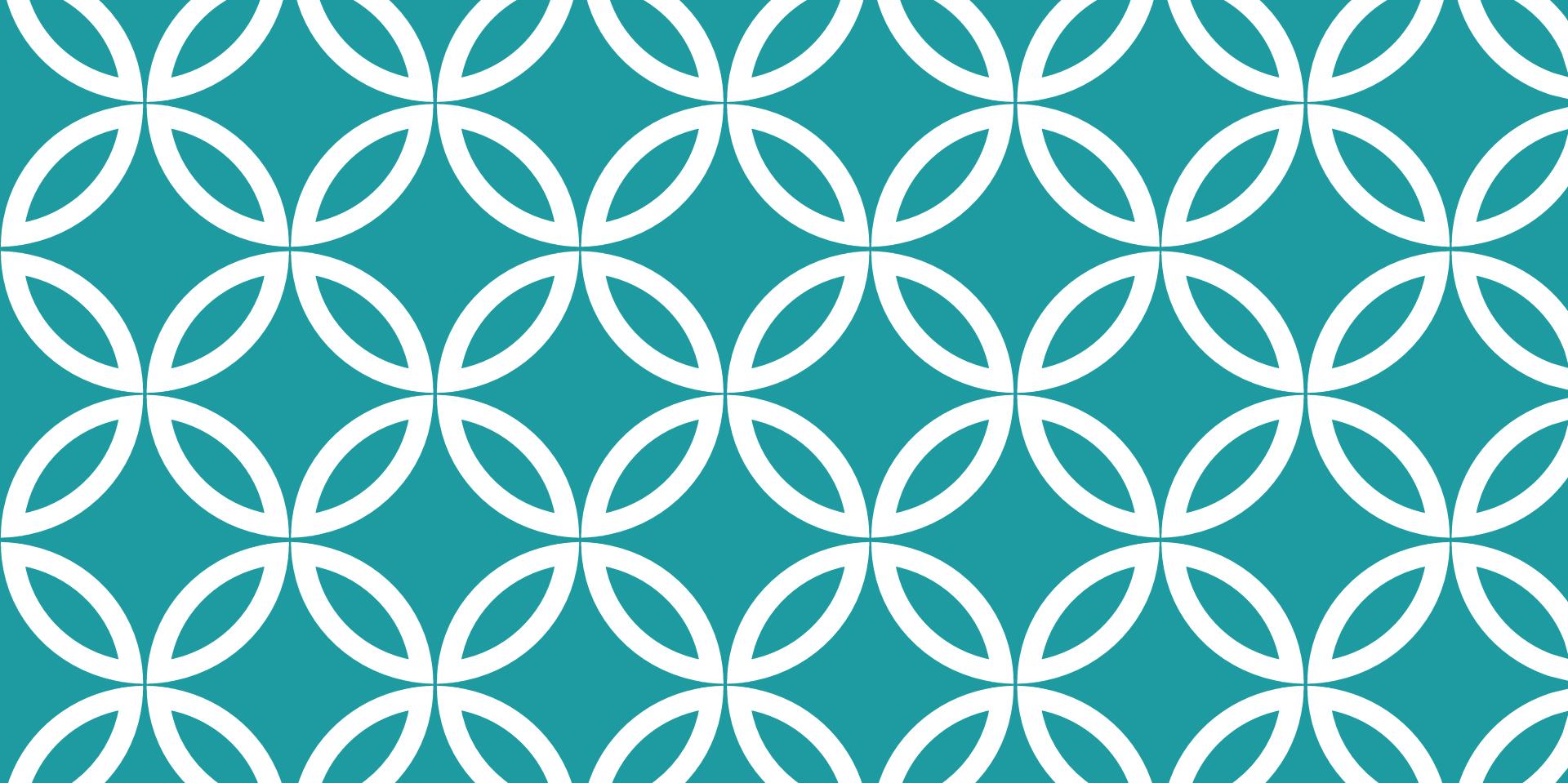
IPv6 Tabla de enrutamiento
=====
Rutas activas:
 Cuando destino de red métrica    Puerta de enlace
   1    306 ::1/128                En vínculo
  13    281 fe80:::/64              En vínculo
  13    281 fe80::88d7:eb89:7591:1ebc/128
                                         En vínculo
   1    306 ff00::/8                En vínculo
  13    281 ff00::/8                En vínculo
=====
Rutas persistentes:
 Ninguno

C:\Users\L00638650>
```

DEFAULT GATEWAY

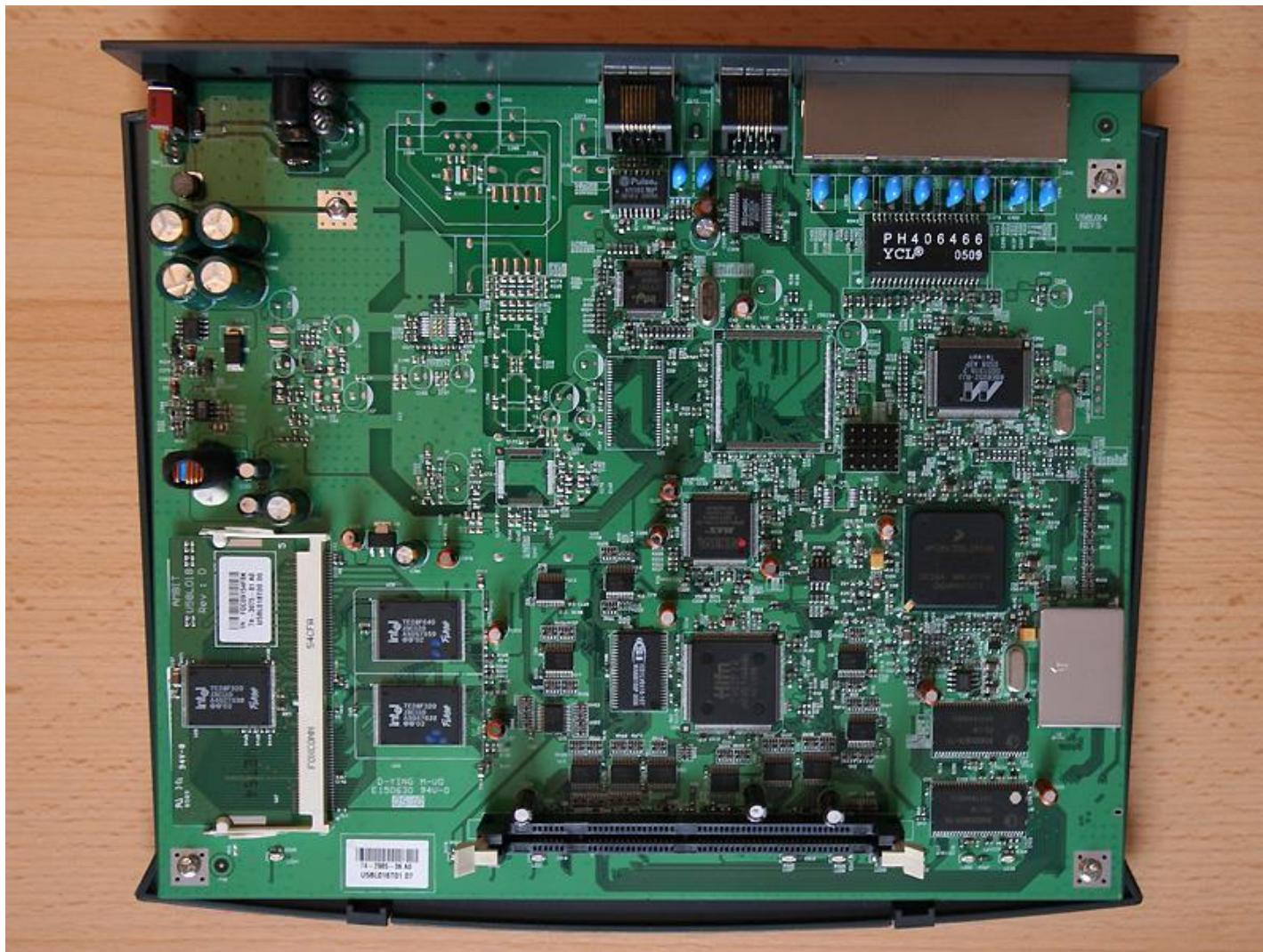
- Es necesaria para enviar un paquete fuera de la red local.
- Es una interfaz del enrutador conectada a la red local.
- Tiene una dirección IP que coincide con la dirección de red de los host.





EL ENRUTADOR

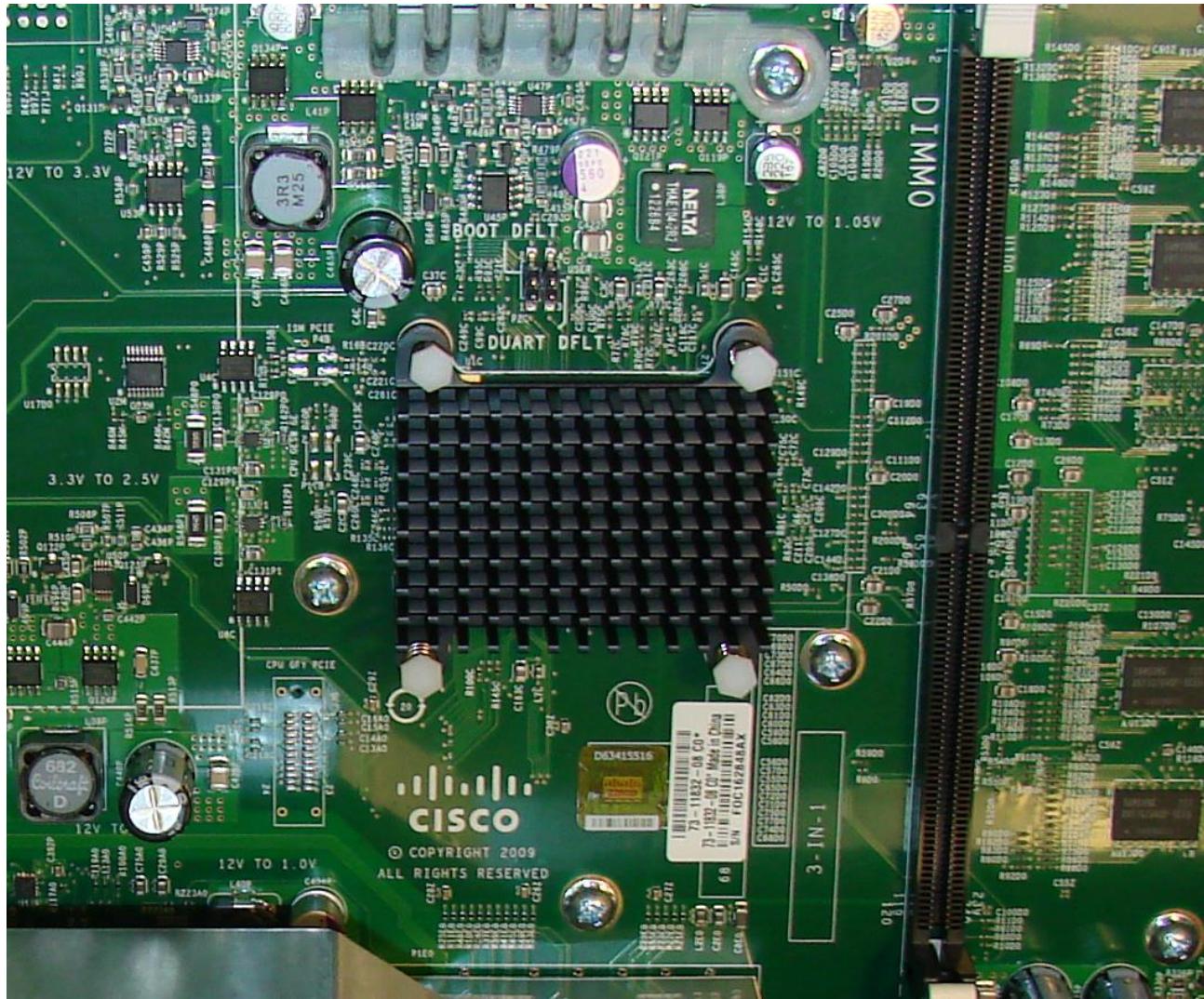
ANATOMÍA



COMO COMPUTADORA



CPU Y OS



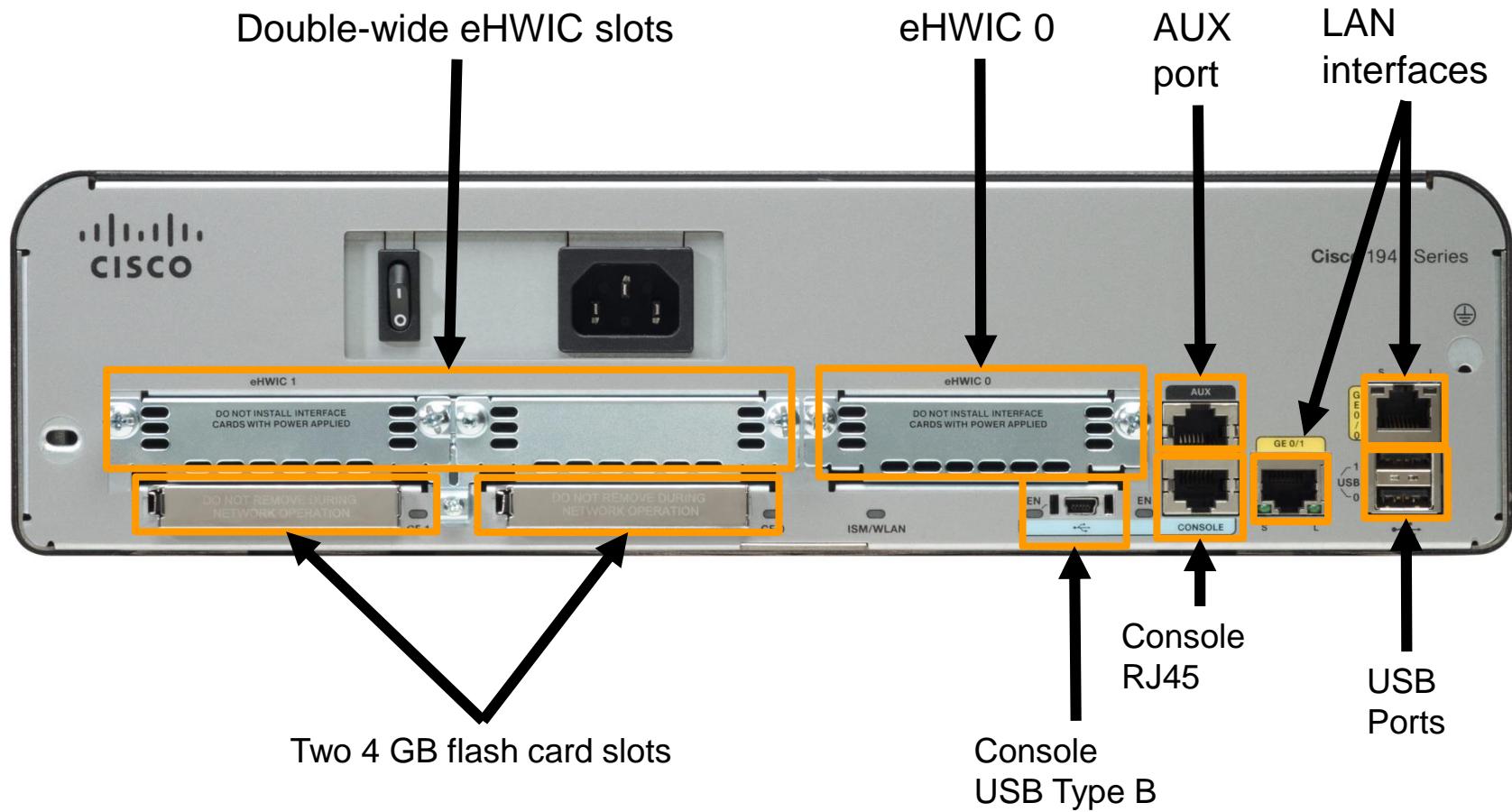
MEMORIA

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	<ul style="list-style-type: none">• Running IOS• Running configuration file• IP routing and ARP tables• Packet buffer
ROM	Non-Volatile	<ul style="list-style-type: none">• Bootup instructions• Basic diagnostic software• Limited IOS
NVRAM	Non-Volatile	<ul style="list-style-type: none">• Startup configuration file
Flash	Non-Volatile	<ul style="list-style-type: none">• IOS• Other system files

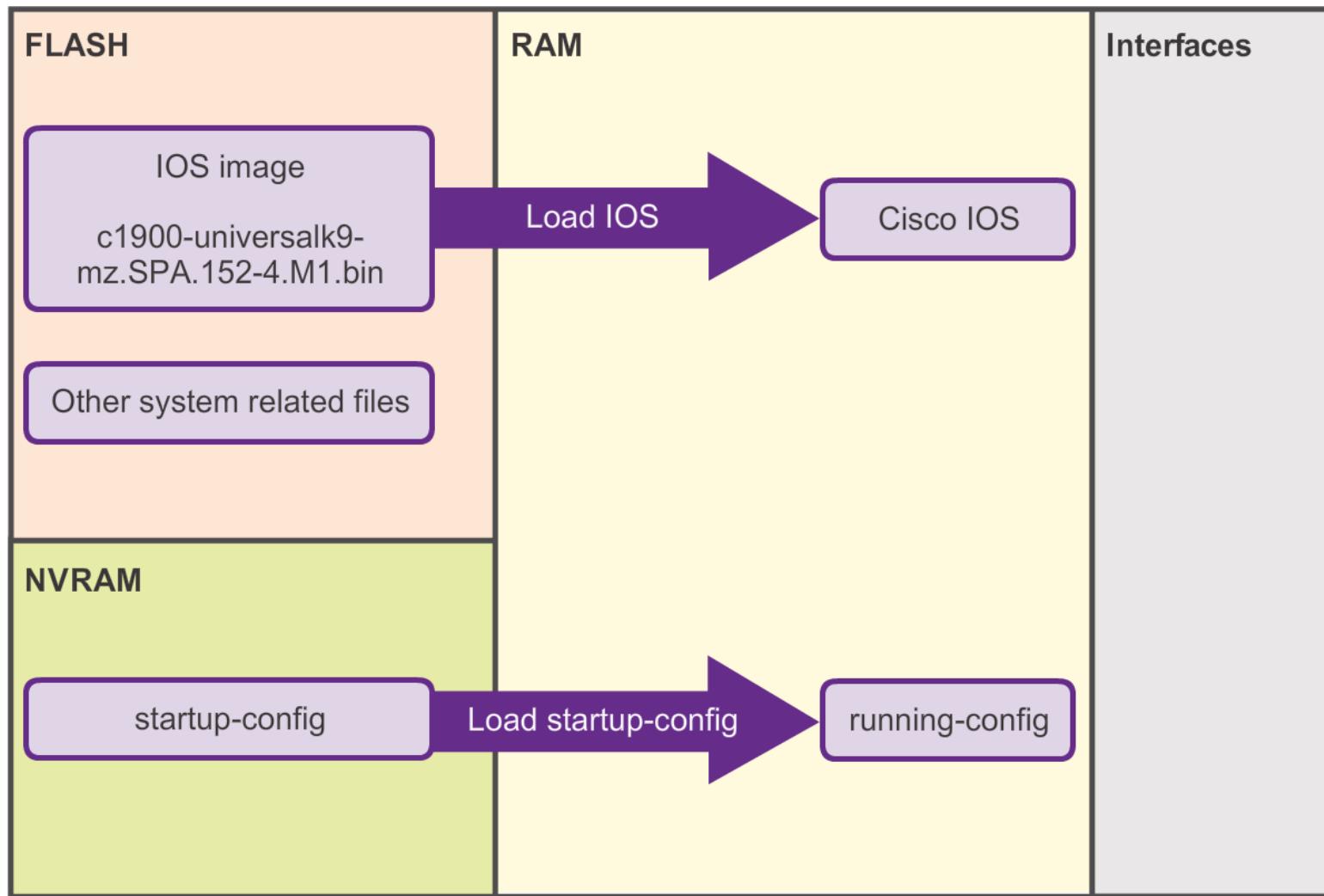
DENTRO DEL ENRUTADOR



INTERFACES

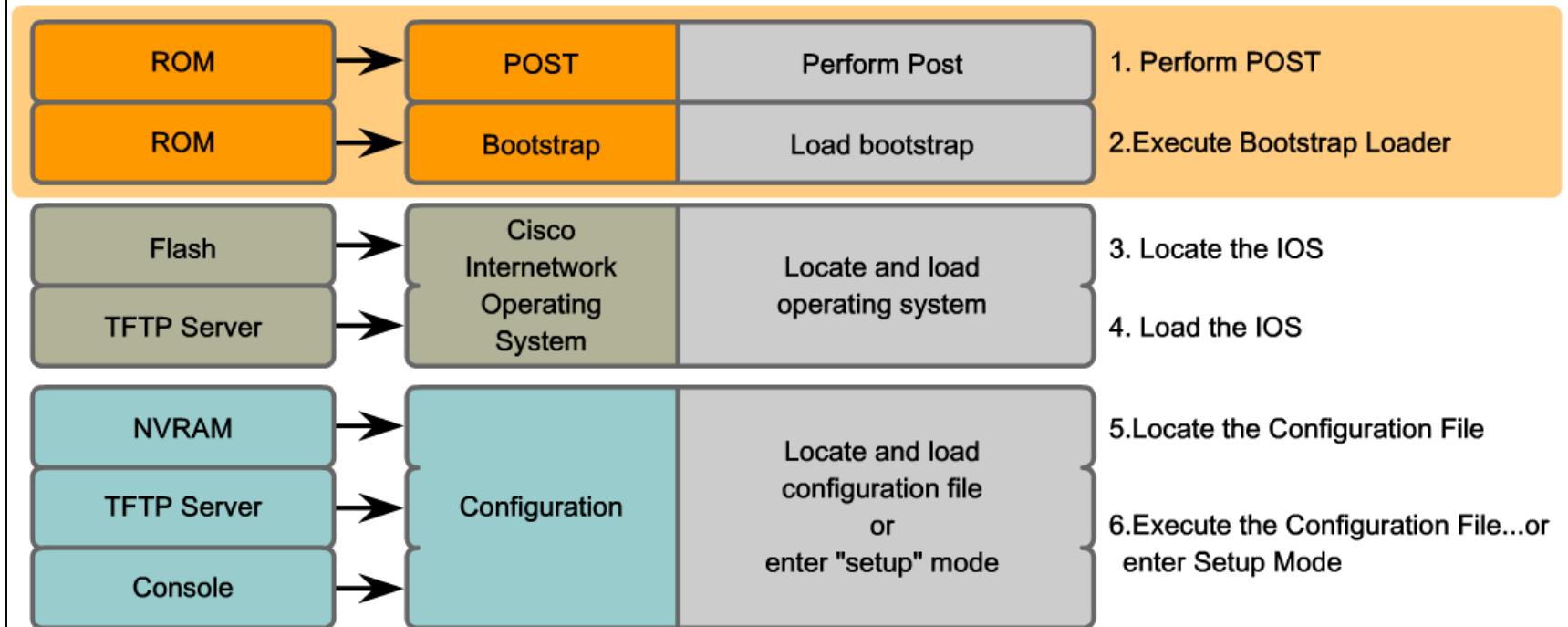


ARCHIVOS BOOTSET



PROCESO BOOTUP

How a Router Boots Up



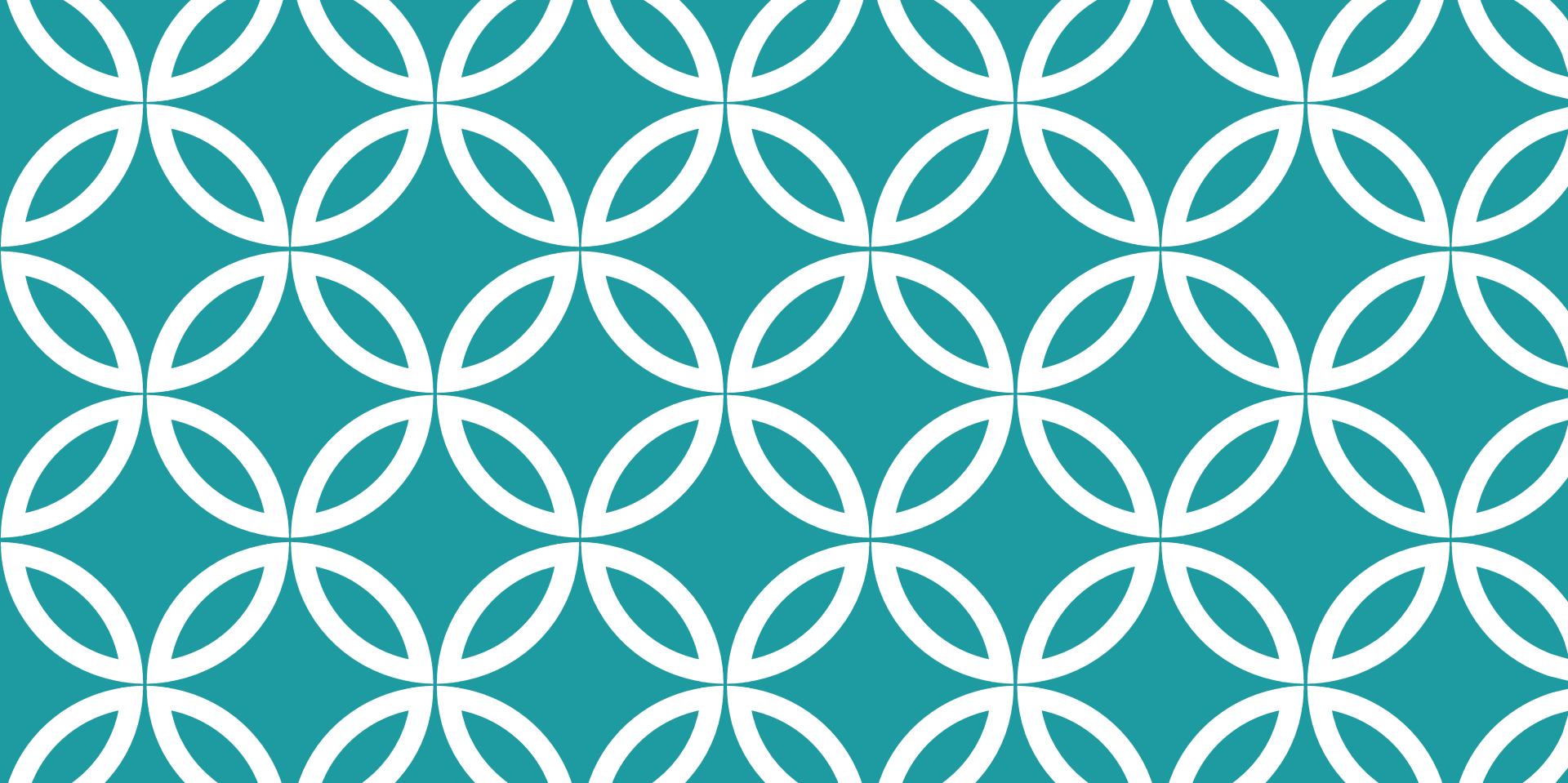
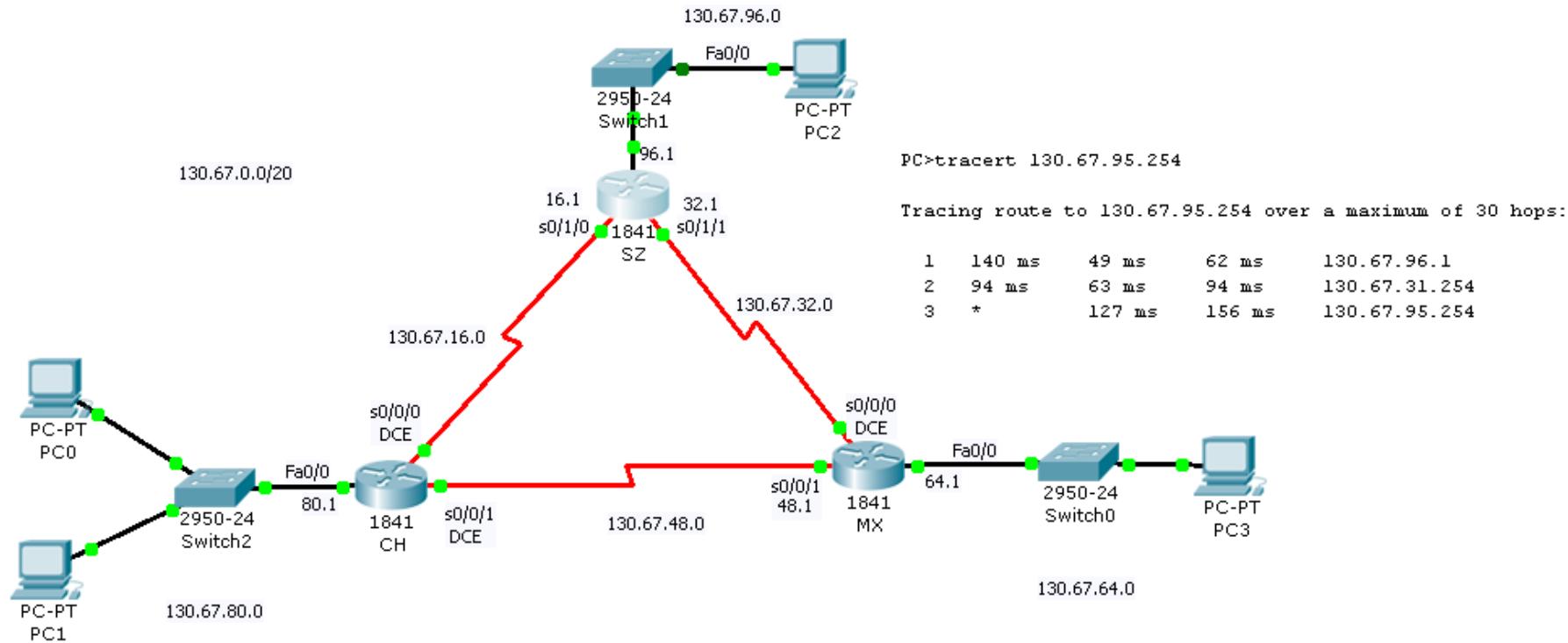


TABLA DE ENRUTAMIENTO DE UN ENRUTADOR



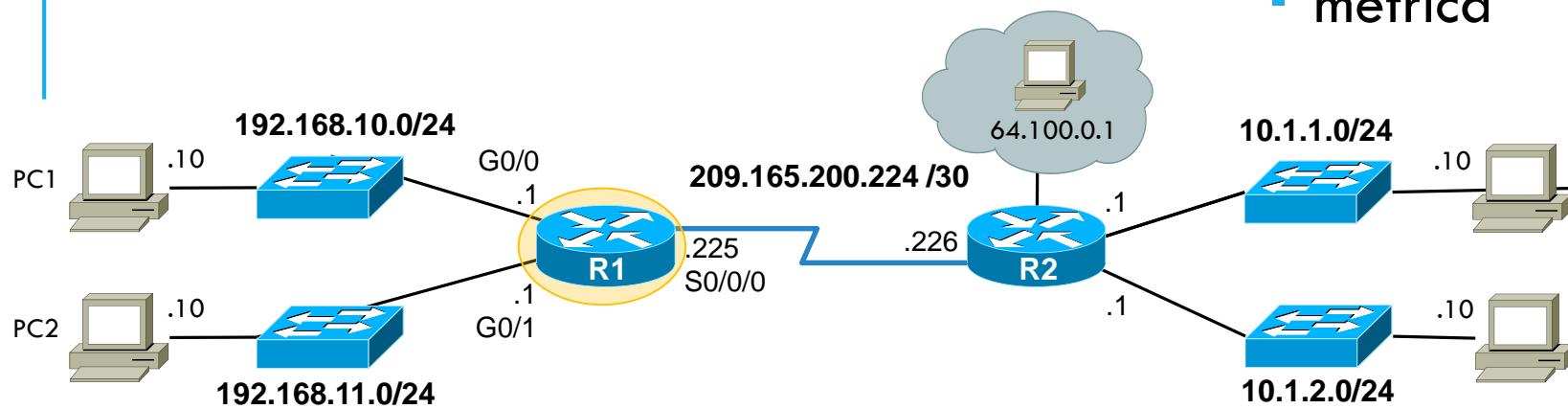
```
SZ#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
130.67.0.0/20 is subnetted, 6 subnets
C     130.67.16.0 is directly connected, Serial0/1/0
C     130.67.32.0 is directly connected, Serial0/1/1
R     130.67.48.0 [120/1] via 130.67.31.254, 00:00:09, Serial0/1/0
          [120/1] via 130.67.47.254, 00:00:09, Serial0/1/1
R     130.67.64.0 [120/1] via 130.67.47.254, 00:00:09, Serial0/1/1
R     130.67.80.0 [120/1] via 130.67.31.254, 00:00:09, Serial0/1/0
C     130.67.96.0 is directly connected, FastEthernet0/0
```

TABLA DE ENRUTAMIENTO

- red de destino
- siguiente salto
- métrica



D	10.1.1.0/24	[90/2170112]	via	209.165.200.226,	00:00:05,	Serial0/0/0
---	-------------	--------------	-----	------------------	-----------	-------------

A	Identificada por el protocolo configurado
B	Red destino
C	Distancia Administrativa
D	Métrica para alcanzar la red remota
E	Siguiente salto
F	Identifica la cantidad de tiempo transcurrido desde que se descubrió la red
G	Identifica la interfaz de salida en el enrutador para llegar a la red de destino

TIPOS DE RUTAS

- **Directamente conectada [C]**
 - Interfaz configurada con una dirección IP y una máscara de subred.
- **Estática [S]**
 - Configurada manualmente por el administrador.
- **Dinámica [R], [D], [O] etc**
 - Aprendida por el protocolo de enrutamiento.
- **Predeterminada (*gateway de último recurso*) [S*]**
 - Tiene la dirección 0.0.0.0 y es utilizada en caso de no existir una ruta para el paquete

PROTOCOLOS DE ENRUTAMIENTO

RIP (Routing Information Protocol)

- Utiliza el conteo de saltos como métrica para la selección de rutas.
- Si el conteo de saltos de una red es mayor de 15, el RIP no puede suministrar una ruta para esa red.

EIGRP (Enhanced Interior Gateway Routing Protocol)

- Métricas: ancho de banda, retardo, carga, confiabilidad y MTU.

OSPF (Open Shortest Path First)

- Métrica: costo.

EJEMPLOS

```
R 10.0.0.0/8 [120/1] via 100.0.0.1, 00:00:07, Serial0/2
R 20.0.0.0/8 [120/1] via 101.0.0.2, 00:00:09, Serial0/1
R 30.0.0.0/8 [120/1] via 102.0.0.2, 00:00:10, Serial1/1
C 100.0.0.0/8 is directly connected, Serial0/2
C 101.0.0.0/8 is directly connected, Serial0/1
C 102.0.0.0/8 is directly connected, Serial1/1
S 192.0.0.0/24 [1/0] via 200.0.0.1
S 193.0.0.0/24 [1/0] via 202.0.0.2
S 194.0.0.0/24 [1/0] via 201.0.0.2
C 200.0.0.0/24 is directly connected, Serial0/0
C 201.0.0.0/24 is directly connected, Serial1/0
C 202.0.0.0/24 is directly connected, Serial0/3
```

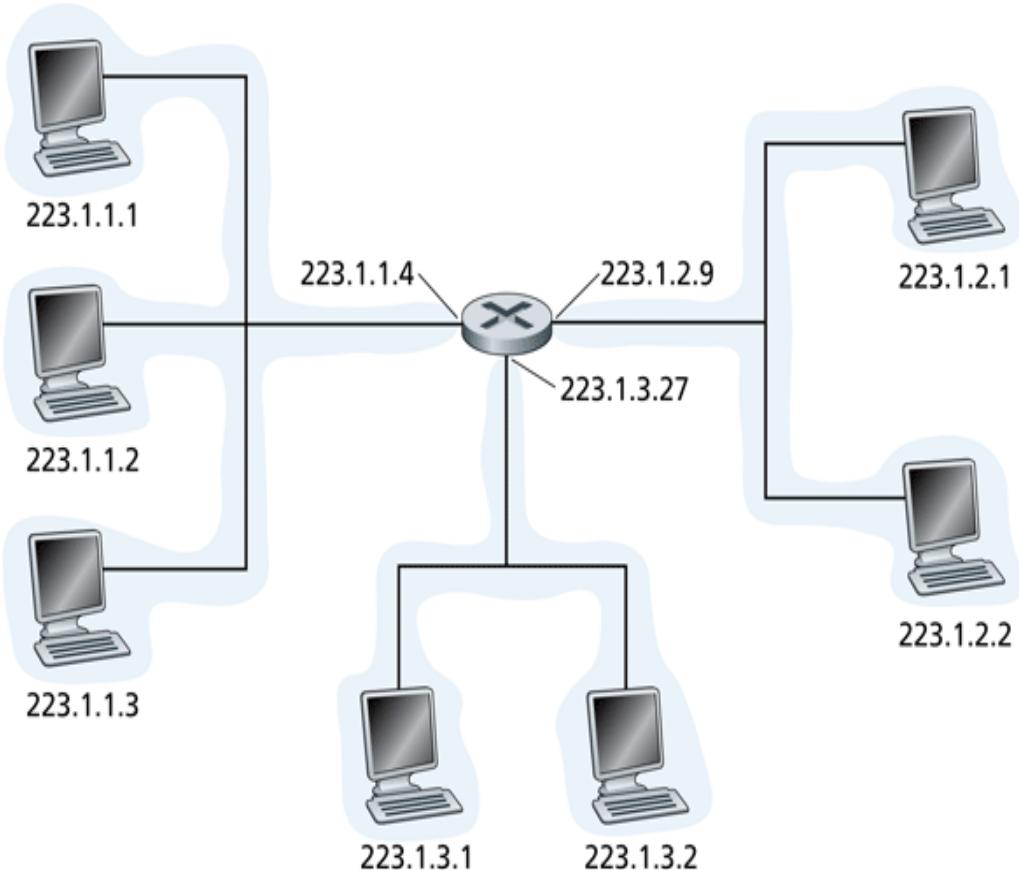
```
R 10.0.0.0/8 [120/2] via 101.0.0.1, 00:00:29, Serial0/0
C 20.0.0.0/8 is directly connected, FastEthernet1/0
R 30.0.0.0/8 [120/2] via 101.0.0.1, 00:00:29, Serial0/0
R 100.0.0.0/8 [120/1] via 101.0.0.1, 00:00:29, Serial0/0
C 101.0.0.0/8 is directly connected, Serial0/0
R 102.0.0.0/8 [120/1] via 101.0.0.1, 00:00:29, Serial0/0
C 193.0.0.0/24 is directly connected, FastEthernet0/0
C 202.0.0.0/24 is directly connected, Serial0/1
S* 0.0.0.0/0 [1/0] via 202.0.0.1
```

COMPARACIÓN

	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Por lo general es independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Se requiere de un conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere la intervención del administrador
Escalamiento	Adecuado para las topologías simples y complejas	Adecuada para topologías simples
Seguridad	Es menos seguro	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

DIRECCIONAMIENTO IPV4

- **Dirección IP:** identificador de 32-bits a un host o *interfaz*.
- **interfaz:** conexión entre host o enrutador y enlace físico.
 - enrutador típicamente tiene múltiples interfaces.
 - host puede tener múltiples interfaces.
 - Direcciones IP están asociadas a cada interfaz.



223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

NOTACIÓN

Binaria

- Para hacer más legible la dirección en esta notación, se agrupan los 32 bits en 4 octetos.

10000000 00001011 00000011 00011111

Decimal

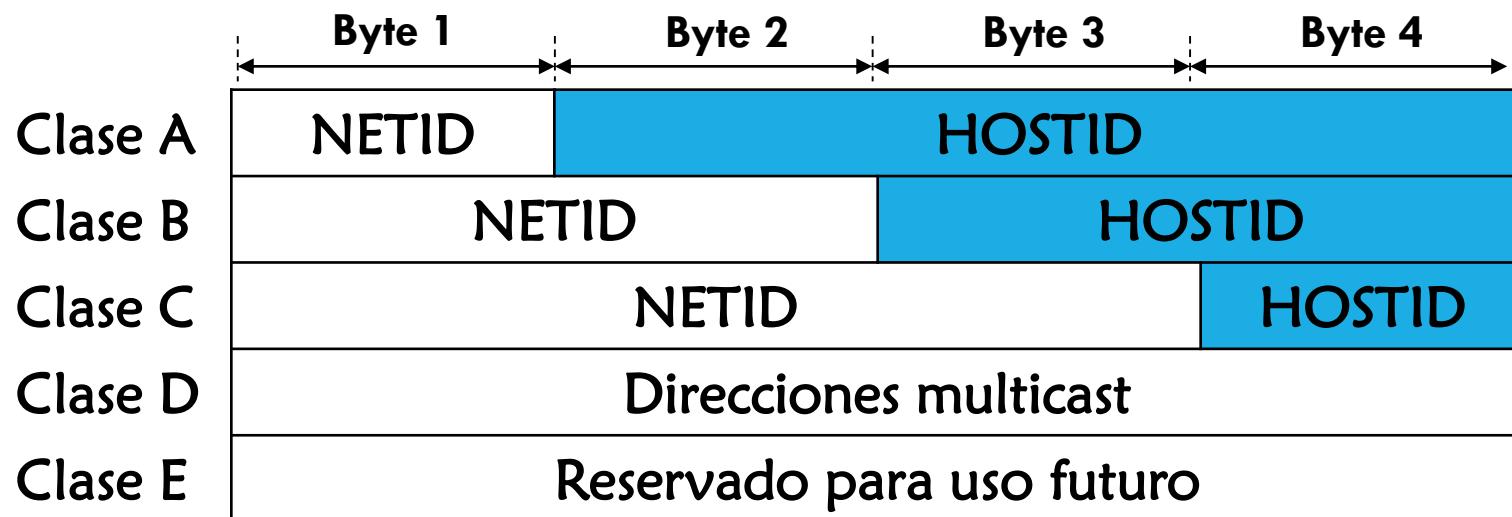
- Para hacer más compacta y legible la dirección, usualmente se utiliza esta notación.

128.11.3.31

Nota: el valor mínimo en decimal para cada octeto es de 0 mientras que el máximo es de 255

IDENTIFICADOR DE RED Y DE NODO

Las direcciones IP de clases A, B y C son divididas en identificador de red (NETID) e identificador de nodo (HOSTID).



TIPOS DE DIRECCIONAMIENTO DE COMUNICACIÓN

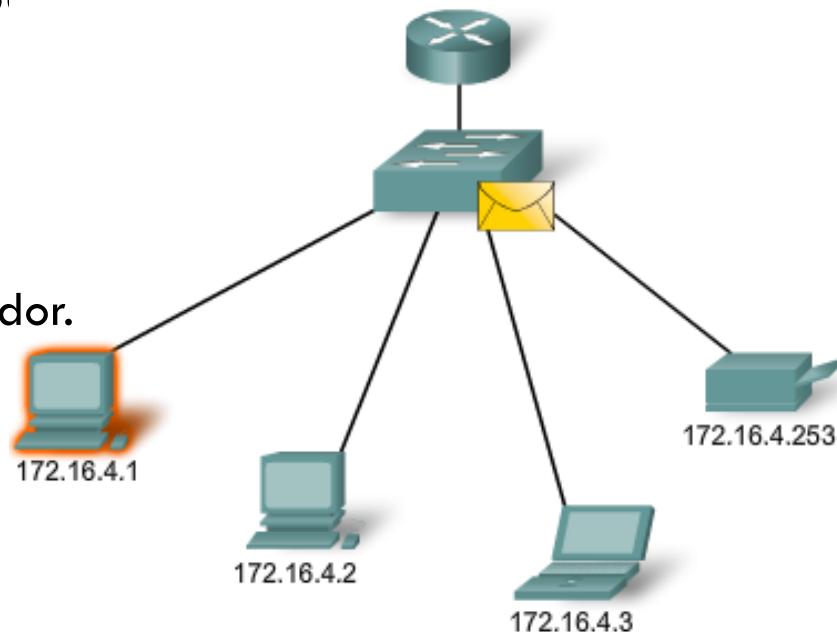
Transmisión Unicas

- Proceso de enviar un paquete individual.

Ejemplos:

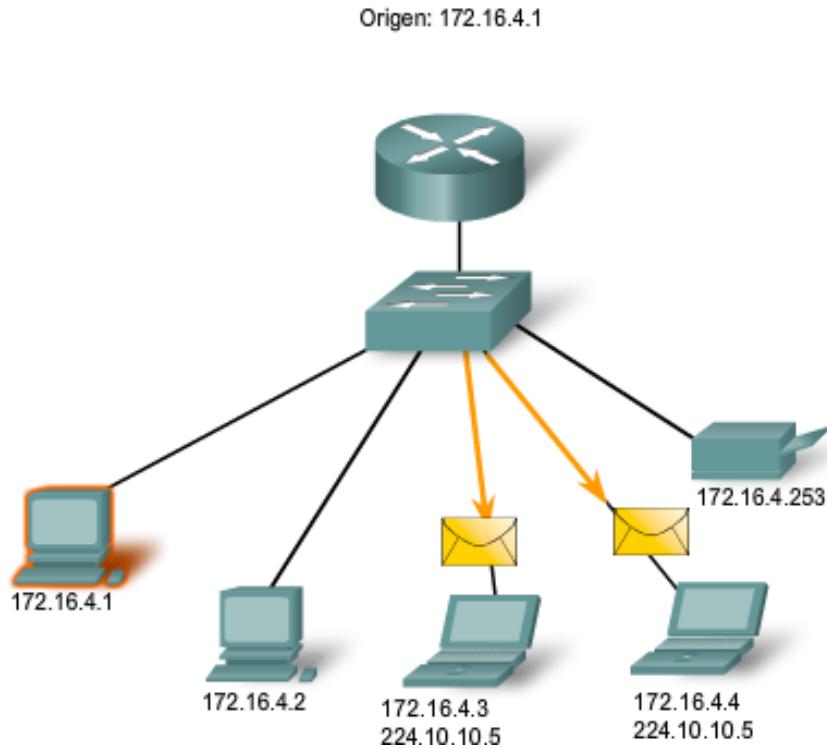
- En una red cliente/servidor.
- En una red P2P.

Origen: 172.16.4.1
Destino: 172.16.4.253



TRANSMISIÓN MULTICAST

Proceso de enviar un paquete de un host a un grupo seleccionado de hosts.



Está diseñado para:

- conservar el ancho de banda.
- reducir el tráfico.

Ejemplos:

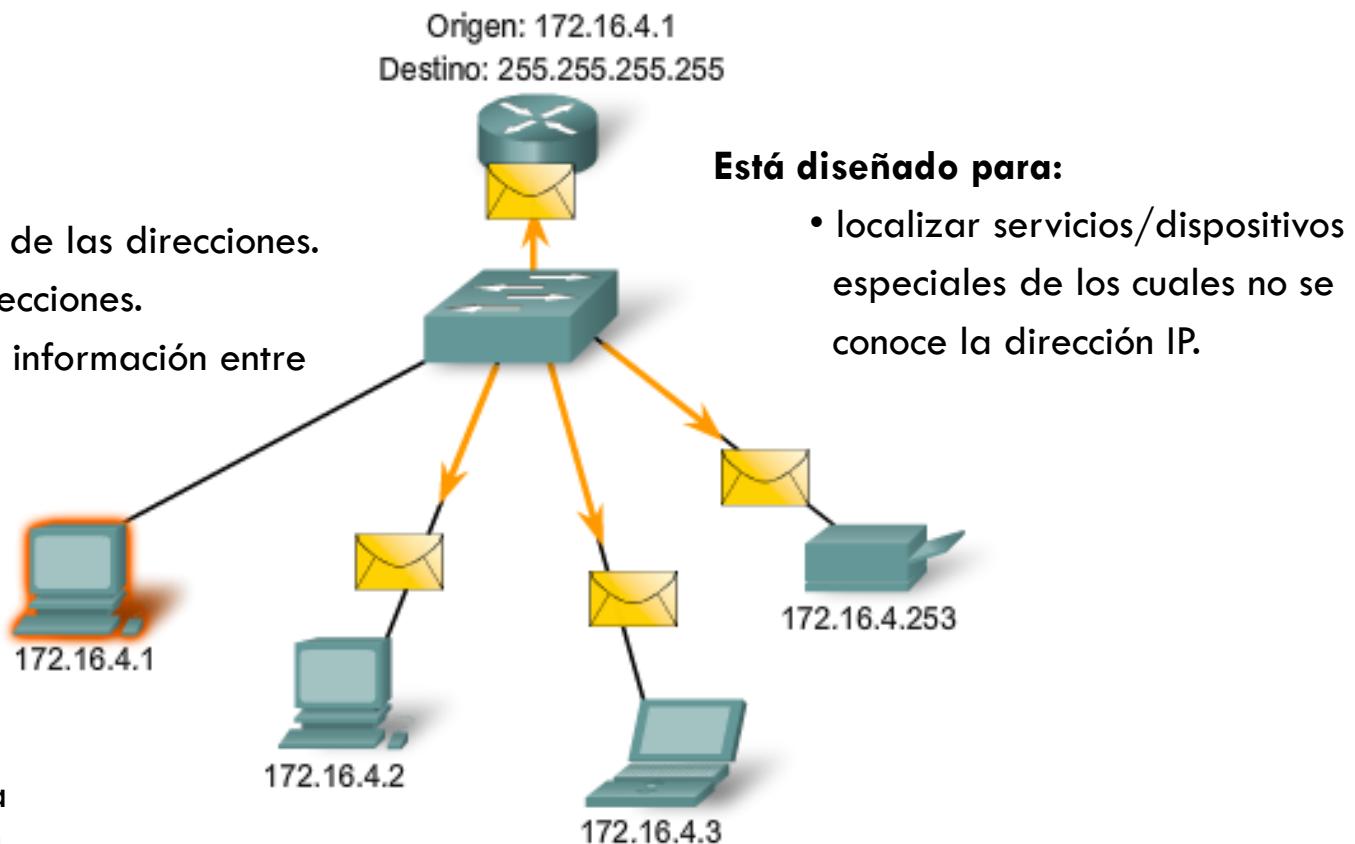
- distribución de video y audio.
- envío de información entre enrutadores.
- distribución de software.

TRANSMISIÓN DE DIFUSIÓN

Proceso de enviar un paquete de un host a TODOS los host, utiliza una dirección especial.

Ejemplos:

- traza un mapa de las direcciones.
- solicitud de direcciones.
- intercambio de información entre enrutadores.



DIRECCIONES IPV4 PARA DIFERENTES PROPÓSITOS

Tipos de direcciones en un rango de red IPv4

- Dirección de red
- Dirección de difusión
- Dirección de host

DIRECCIÓN DE RED

Dirección de red

Red	Host
10 0 0 0	0

00001010 00000000 00000000 00000000

Dirección de broadcast

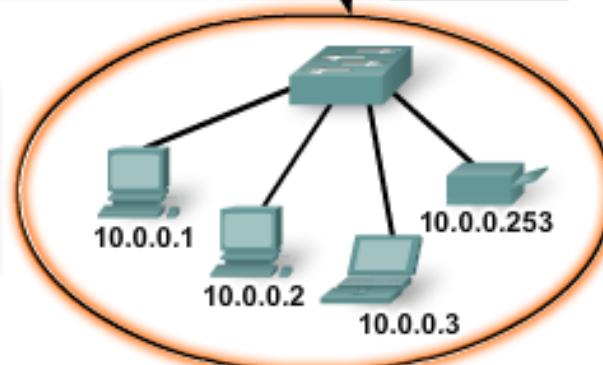
10 0 0 0	255
00001010 00000000 00000000	11111111

Dirección host

Coloque el cursor del mouse aquí para obtener más información.

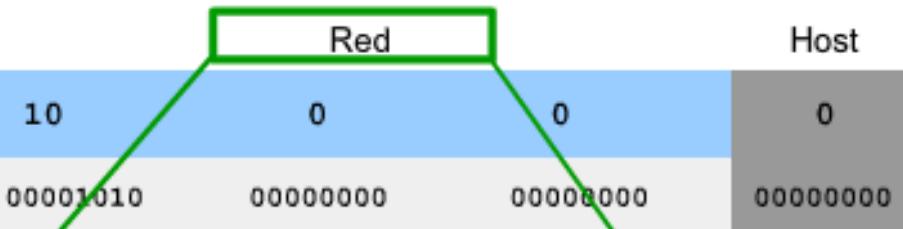
10 0 0 0	1
00001010 00000000 00000000	00000001

10.0.0.0 se utiliza para referirse a la red en su totalidad.
Todos los dispositivos en esta red poseen los mismos bits de dirección de red.



DIRECCIÓN DE DIFUSIÓN

Dirección de red



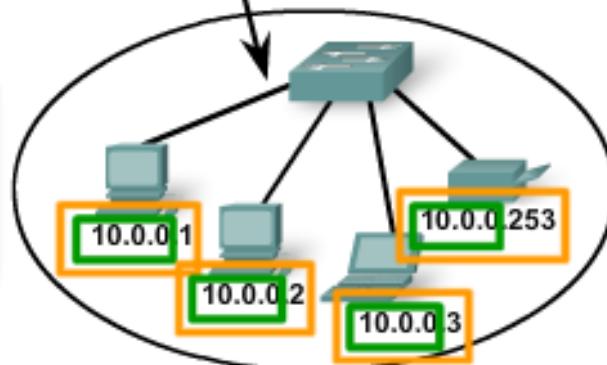
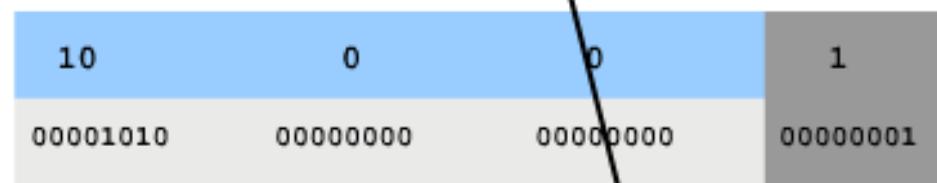
Dirección de broadcast



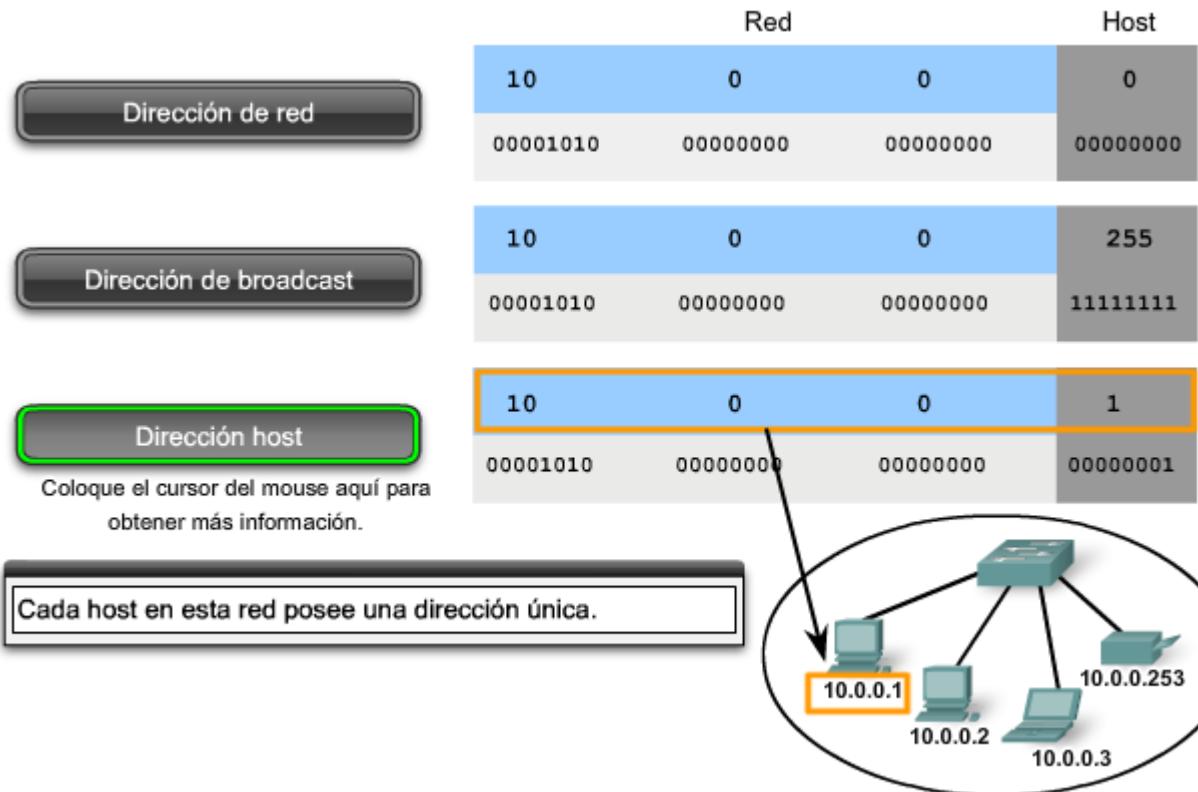
Dirección host

Coloque el cursor del mouse aquí para obtener más información.

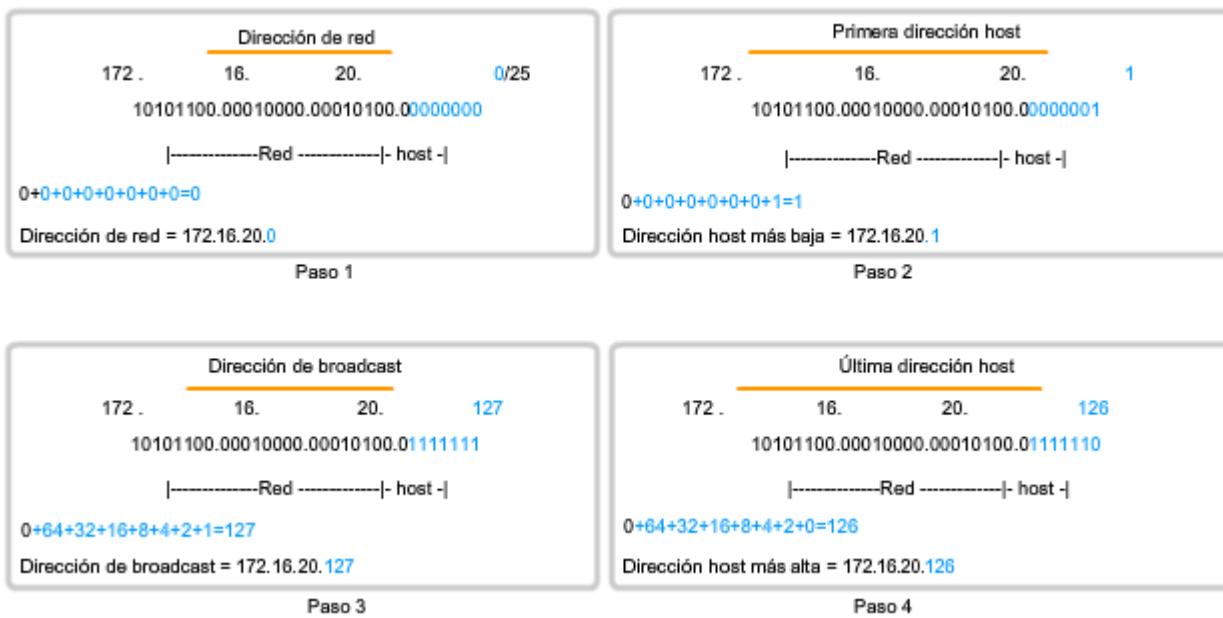
La dirección de broadcast se utiliza para enviar paquetes a cada host en la red que comparta la misma porción de red de la dirección.



DIRECCIÓN DE HOST



CÁLCULO DE LAS DIRECCIONES DE HOST, RED Y DIFUSIÓN



PREFIJOS DE RED

¿Cómo se puede saber cuántos bits de esta dirección representan la dirección de red y cuántos la porción de host?

- Respuesta: por medio de la máscara prefijo.

Esta longitud de prefijo es el número de bits de la dirección que proporcionan la porción de red y se escribe en formato de barra inclinada (notación CIDR).



Red	Dirección de red Todos los bits de hosts (rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.128	172.16.4.127
Representación binaria 25 bits de red	10101100.00010000.00000100.00000000 0.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.01111110	10101100.00010000.00000100.01111111 11
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED
PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE
BROADCAST PARA CADA
PREFIJO

126 hosts

DIFERENTE CANTIDAD DE HOSTS PARA CADA
PREFIJO

MÁSCARA DE SUBRED

Es un valor de 32 bits que especifica la porción de red.

Se crea colocando un 1 binario en cada posición de bit apropiada que representa un bit de red de la dirección, se coloca un 0 binario en el resto de las posiciones.

Dirección IP: 10011100.10011010.01010001.00111000

Máscara de subred: 11111111.11111111.11111111.11110000

RANGO DE DIRECCIONES EXPERIMENTALES

Tipo de dirección	Uso	Rango de direcciones IPv4 reservadas	RFC
Dirección host	utilizada en hosts IPv4	De 0.0.0.0 a 223.255.255.255	790
Dirección multicast	utilizada en grupos multicast en una red local	De 224.0.0.0 a 239.255.255.255	1700
Direcciones experimentales	<ul style="list-style-type: none">utilizada para investigación o experimentaciónactualmente no se puede utilizar para los hosts en las redes IPv4	De 240.0.0.0 a 255.255.255.254	1700 3330

Direcciones públicas y privadas

Direcciones públicas

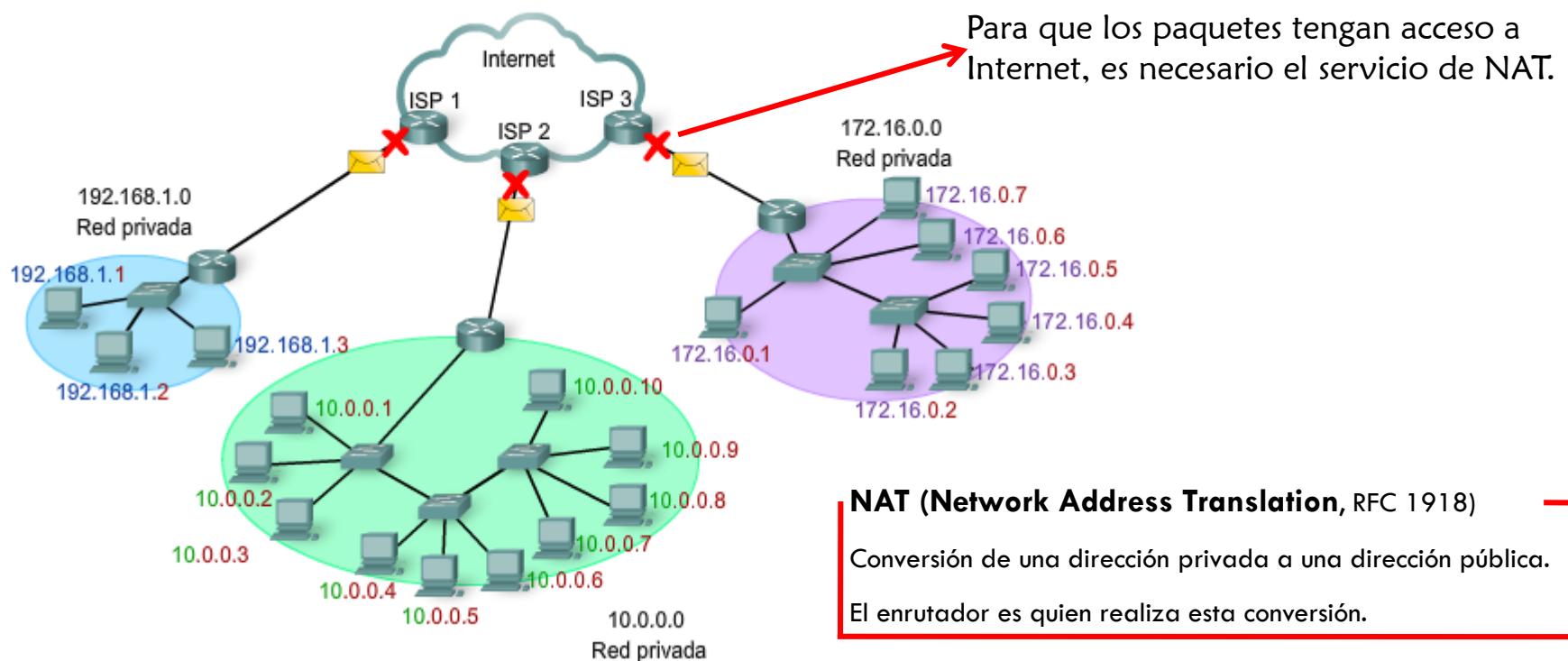
La mayoría de las direcciones unicast IPv4 son direcciones públicas.

Estas direcciones son diseñadas para poder acceder a Internet.

DIRECCIONES PRIVADAS

Bloque de direcciones:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)



DIRECCIONES IP UNICAST ESPECIALES

Ruta predeterminada

- 0.0.0.0 dirección del tipo “alcanzar todo”.
- Se utiliza cuando el paquete no tiene una ruta disponible.
- Esta dirección también reserva el bloque de direcciones

0.0.0.0-0.255.255.255

Dirección de loopback

- 127.0.0.1 dirección local del host.
- Se utiliza para probar la configuración de TCP/IP.
- Esta dirección también reserva el bloque de direcciones

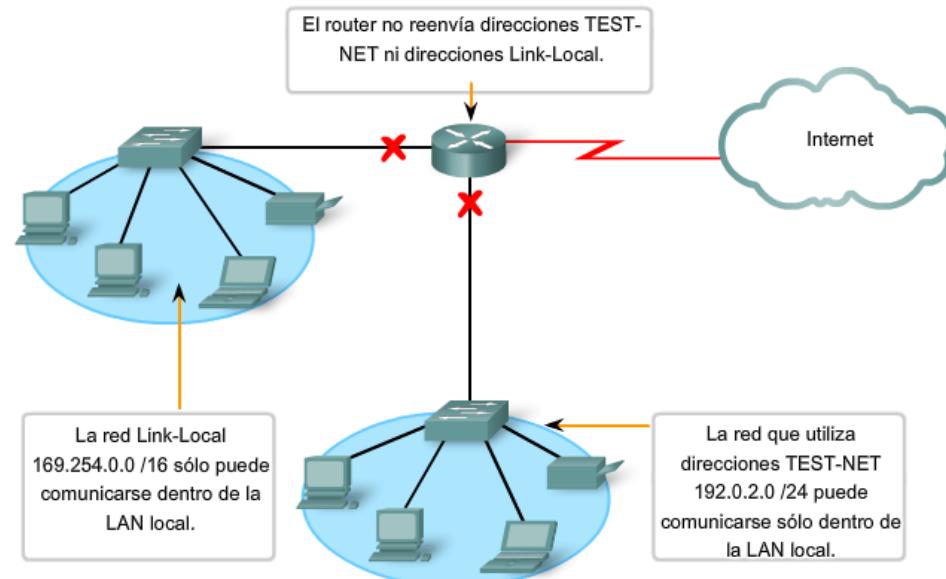
127.0.0.0-127.255.255.255

Dirección de enlace local

- Direcciones 169.254.0.0-169.254.255.255.
- El sistema operativo asigna automáticamente estas direcciones cuando no hay disponible una dirección IP.
- Se pueden utilizar en una red peer-to-peer (P2P) al no ser asignadas por DHCP.
- Estas direcciones no proporcionan servicio fuera de la red local.

Direcciones test-net

- Direcciones 192.0.2.0-192.0.2.155.
- Utilizadas para fines de enseñanza y aprendizaje.



DIRECCIONAMIENTO CLASSFUL

El espacio de direccionamiento IP se divide en:

Clase de direcciones	1er rango del octeto (decimal)	1eros bits del octeto (los bits verdes no cambian)	Partes de las direcciones de red(N) y de host(H)	Máscara de subred predeterminada (decimal y binaria)	Número de posibles redes y hosts por red
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16,777,214 hosts por red (2^{24-2})
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 redes (2^{14}) 65,534 hosts por red (2^{16-2})
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 redes (2^{21}) 254 hosts por red (2^{8-2})
D	224-239	11000000-11011111	ND (multicast)		
E	240-255	11110000-11111111	ND (experimental)		

ASIGNACIÓN DE DIRECCIONES

Planificación del direccionamiento de la red

- Evitar la duplicación de direcciones.
 - Un host que intenta usar la misma dirección no podrá comunicarse a través de la red.
- Proporcionar y control el acceso.
 - Si un servidor tiene asignada una dirección aleatoria, es difícil bloquear el acceso.
- Monitorizar la seguridad y el rendimiento.
 - Examinar el tráfico de la red para determinar que dirección IP está generando o recibiendo demasiados paquetes.

DIRECCIONAMIENTO ESTÁTICO O DINÁMICO

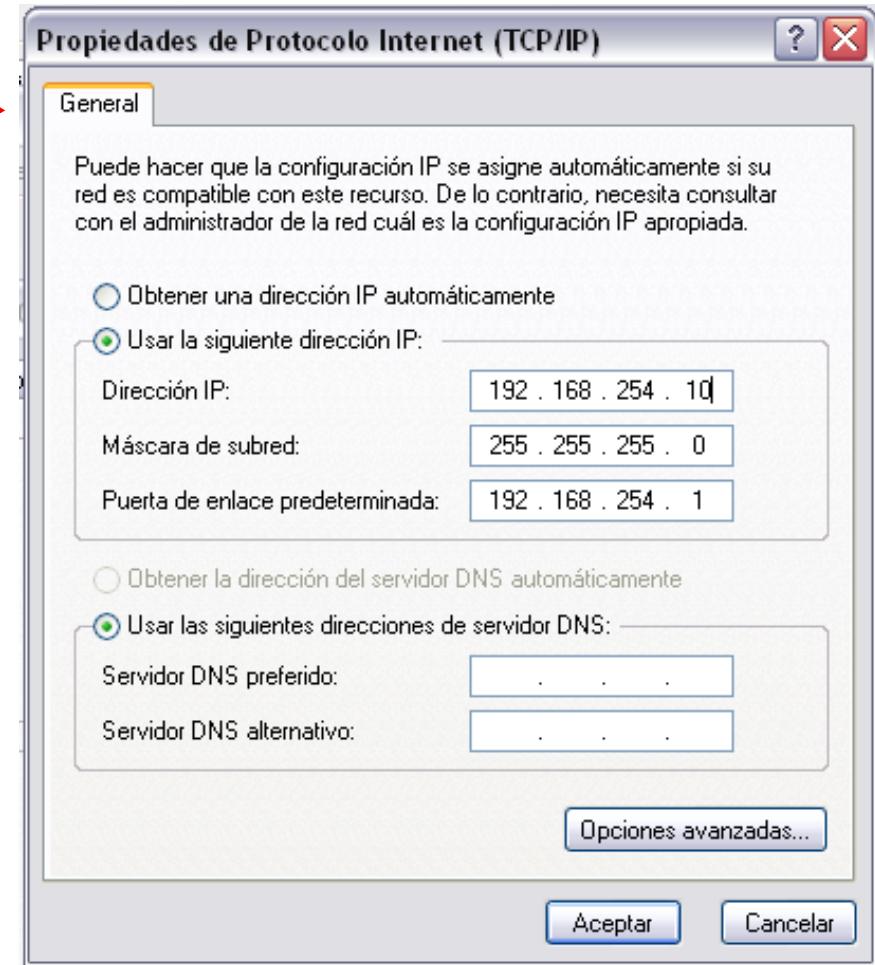
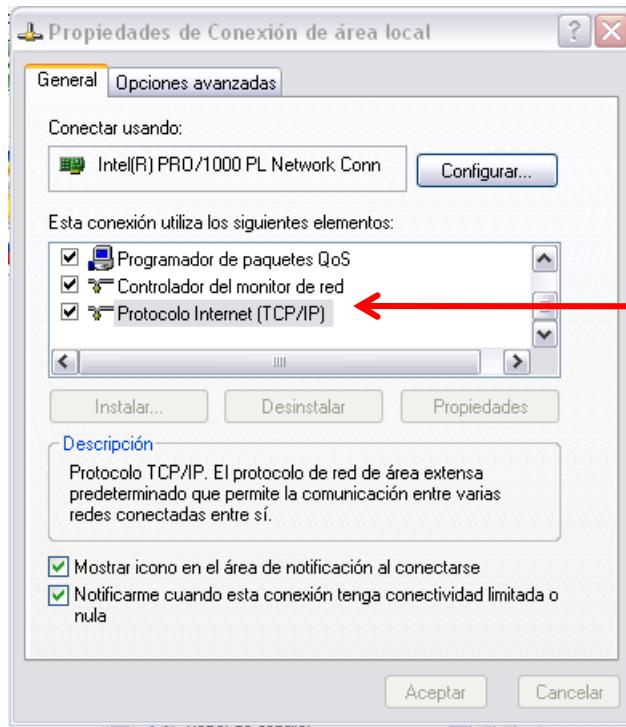
Asignación estática

- El administrador de la red configura manualmente la información de la red para un host.
- Son útiles para impresoras, servidores y otros dispositivos accesibles para los clientes de la red.
- Se tiene un mayor control de los recursos de la red.
- Se debe de mantener una lista exacta de las direcciones IP para no duplicarlas.

Las direcciones estáticas para la interfaz de una computadora basada en

Windows se establece en la pantalla de Propiedades de TCP/IP.

inicio → conectar a → mostrar todas las conexiones → conexión de área local → propiedades



Introducir:

- ✓ Dirección IP
- ✓ Máscara de subred
- ✓ Puerta de enlace predeterminada

CÁLCULO DE DIRECCIONES

¿El host está en mi red?

¿A qué red pertenece este host?

AND: ¿Cuál está en su red?

- Dirección del host más la suma lógica de la máscara de subred.

Dirección host	172	16	132	70
Dirección host binaria	10101100	00010000	10000100	01000110

Operación AND

- 1 and 1 = 1
- 1 and 0 = 0
- 0 and 1 = 0
- 0 and 0 = 0

Máscara de subred binaria	11111111	11111111	11110000	00000000
Dirección de red binaria	10101100	00010000	10000000	00000000
Dirección de red	172	16	128	0

Subneteo

Es fundamental que se conozca el número de bits que se requieren -de la parte de host de cualquier clase- para empezar a crear las subredes.

Para saber cuántos bits se necesitan para crear subredes es necesario que se proporcione una de estas opciones:

- El número de subredes.
- La máscara de subred.
- El esquema para determinar el número de subredes.

Ejemplo 1

Dada la dirección IP 192.168.21.0 se necesitan generar 28 subredes.

¿Qué máscara de subred se deberá utilizar?

Pasos:

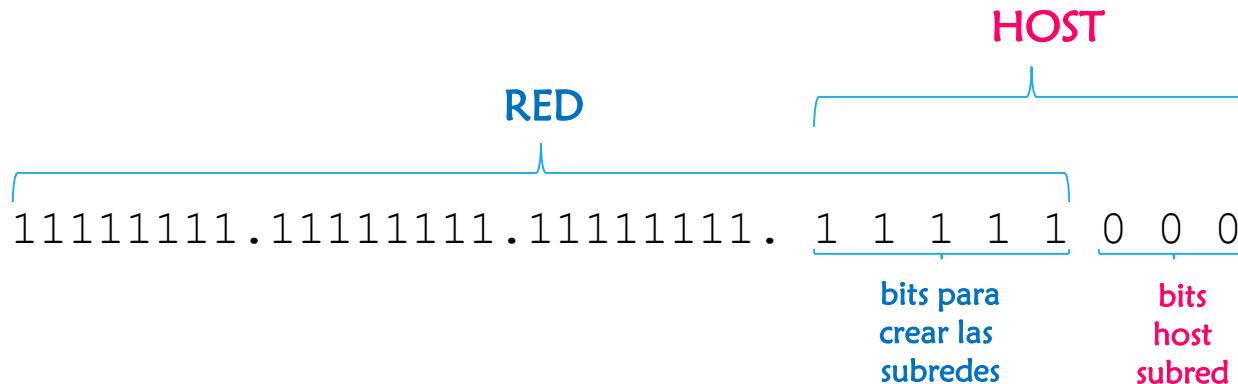
1. ¿A qué clase pertenece la dirección IP 192.168.21.0?
2. ¿Cuál es la máscara determinada de la dirección IP?
3. ¿Cuántos bits se necesitan para representar el número 28, que son las subredes que se necesitan generar?

Por lo tanto:

La máscara determinada para la red 192.168.21.0 es:

255 . 255 . 255 . 0
11111111.11111111.11111111. 00000000
RED HOST

Como son 5 bits los necesarios para representar el número 28, entonces tomaremos esos 5 bits de la parte de host de la clase C.



Por lo tanto, la máscara de subred será:

255.255.255. 1 1 1 1 1 0 0 0
| | | | |
| | | | | 8
| | | | | 16
| | | | | 32
| | | | | 64
| | | | | 128

255.255.255.248

Ejemplo 2

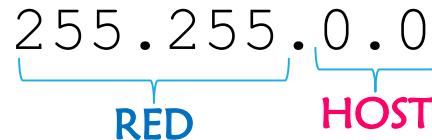
¿Cuál es la dirección de difusión de la dirección
de subred

172.16.99.99 con máscara de subred de
255.255.192.0?

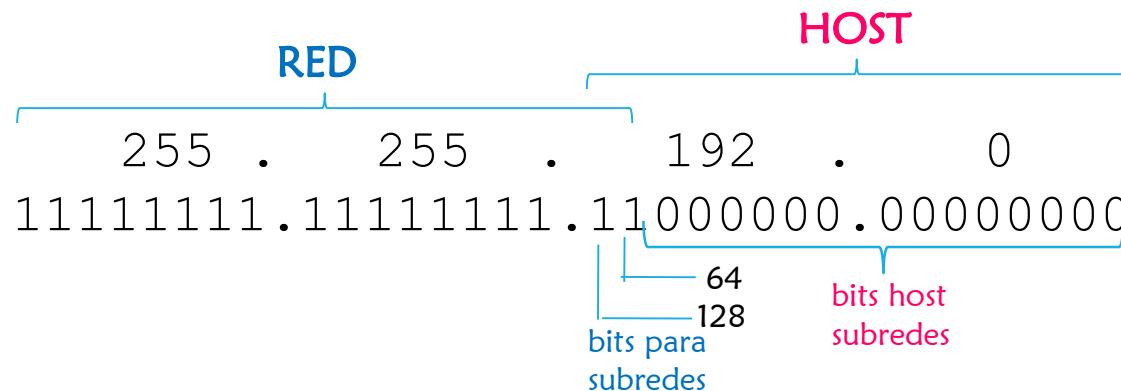
Pasos:

1. ¿A qué clase pertenece la dirección IP 172.16.99.99?
2. ¿Cuál es la máscara determinada de la dirección IP?
3. ¿Cuántos bits se nos están prestando de la parte de host de la clase para crear las subredes?

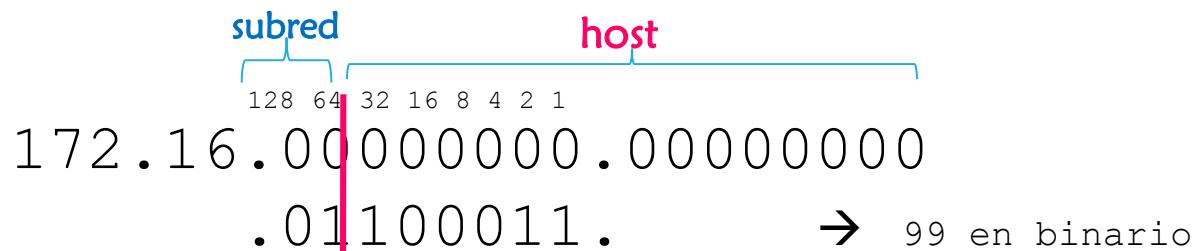
La máscara determinada para la red 172.16.99.99 es:



La máscara de subred dada es:

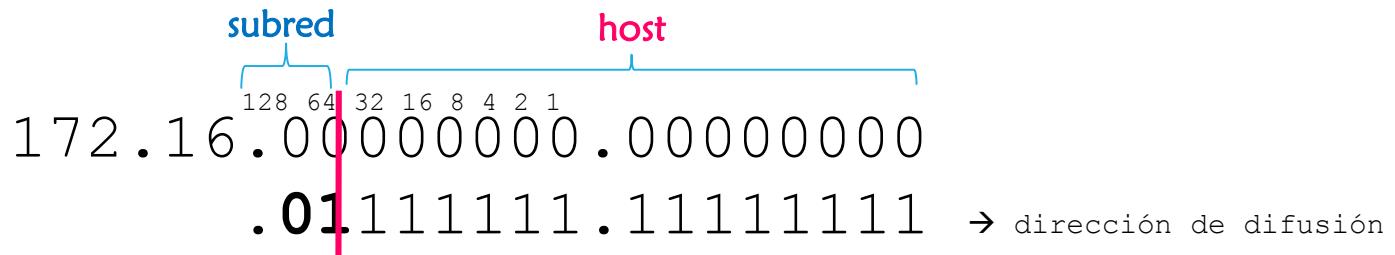


Identificando cuantos bits son para crear subredes y cuantos bits son para host, es necesario ahora identificar en qué subred se encuentra la dirección IP 172.16.99.99.



Por lo tanto, la dirección IP 172.16.99.99 pertenece a la subred 1 con dirección IP 172.16.64.0.

Ahora para obtener la dirección de difusión de la subred 1, se hará lo siguiente:

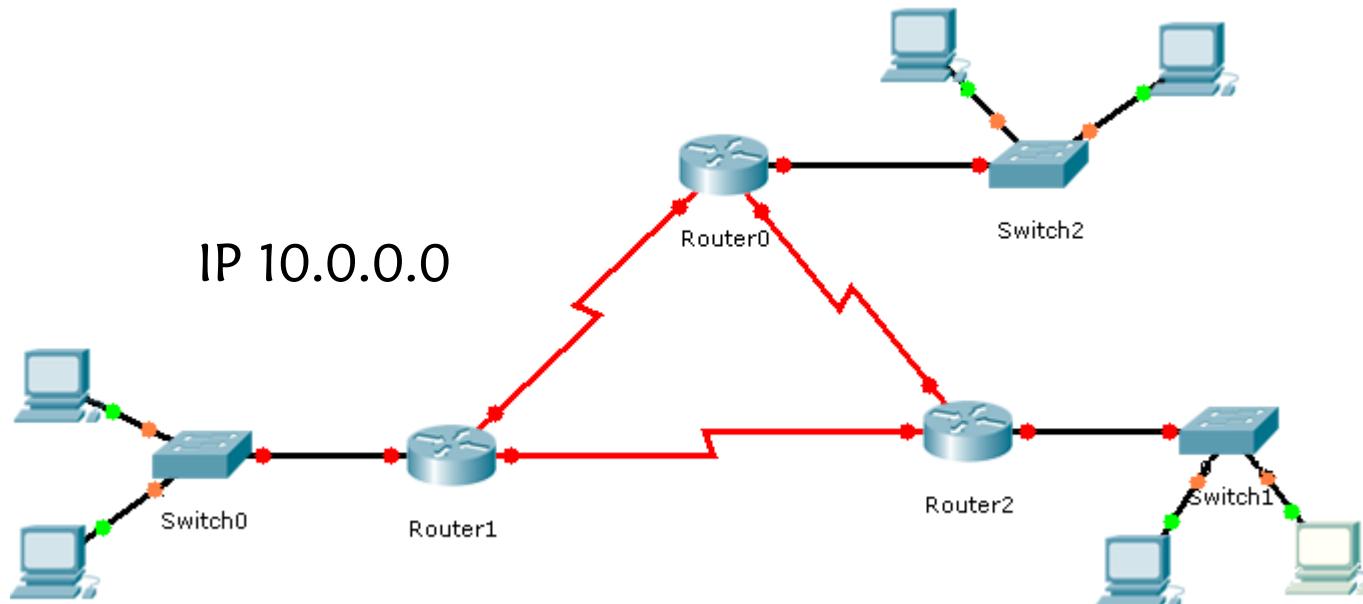


Por lo tanto, la dirección de difusión de la subred 1 es:

172.16.127.255/18

Ejemplo 3

¿Cuál será la dirección IP de la subred 3 del siguiente esquema?



Pasos:

1. ¿A qué clase pertenece la dirección IP 10.0.0.0?
2. ¿Cuál es la máscara determinada de la dirección IP?
3. ¿Cuántas subredes existen en el esquema?

La máscara determinada para la red 10.0.0.0 es:

255.0.0.0

El número de subredes que existen en el diagrama son 6. Por lo tanto, necesitamos 3 bits de la parte de host para crear las subredes.

The diagram illustrates a 32-bit IP address structure. It consists of four bytes represented by black digits (255, 0, 0, 0) followed by three dots, and then four more black digits (0, 0, 0, 0). Above the first byte, the word "RED" is written in blue, with a blue bracket underneath it. Above the fourth byte, the word "HOST" is written in red, with a blue bracket underneath it. Below the second byte, the word "subred" is written in blue, with a blue bracket underneath it. Below the fifth byte, the word "host" is written in red, with a blue bracket underneath it.

Una vez identificados los bits, convertir el número de la subred que nos piden en binario utilizando esos tres dígitos de la subred.

10.0000000.0000000.0000000
011 → subred número 3

Por lo tanto, la dirección IP de la subred 3 es:

10.96.0.0

Calcular la Cantidad de Subredes y Hosts por Subred

Cantidad de Subredes es igual a: $2^N - 2$, donde "N" es el número de bits "prestados" a la porción de Host y "-2" porque la primer subred y la última subred no son utilizables ya que contienen la dirección de la red y difusión respectivamente.

Cantidad de Hosts x Subred es igual a: $2^M - 2$, donde "M" es el número de bits disponible en la porción de host y "-2" es debido a que toda subred debe tener su propia dirección de red y su propia dirección de difusión.

EJERCICIOS



COMPROBACIÓN DE LA CAPA DE RED

Ping

- Comando para probar conectividad entre los hosts.
- Utiliza un datagrama de solicitud de eco ICMP.

Ping 127.0.0.1: comprobación de la pila local

- Comprueba la configuración interna de IP.

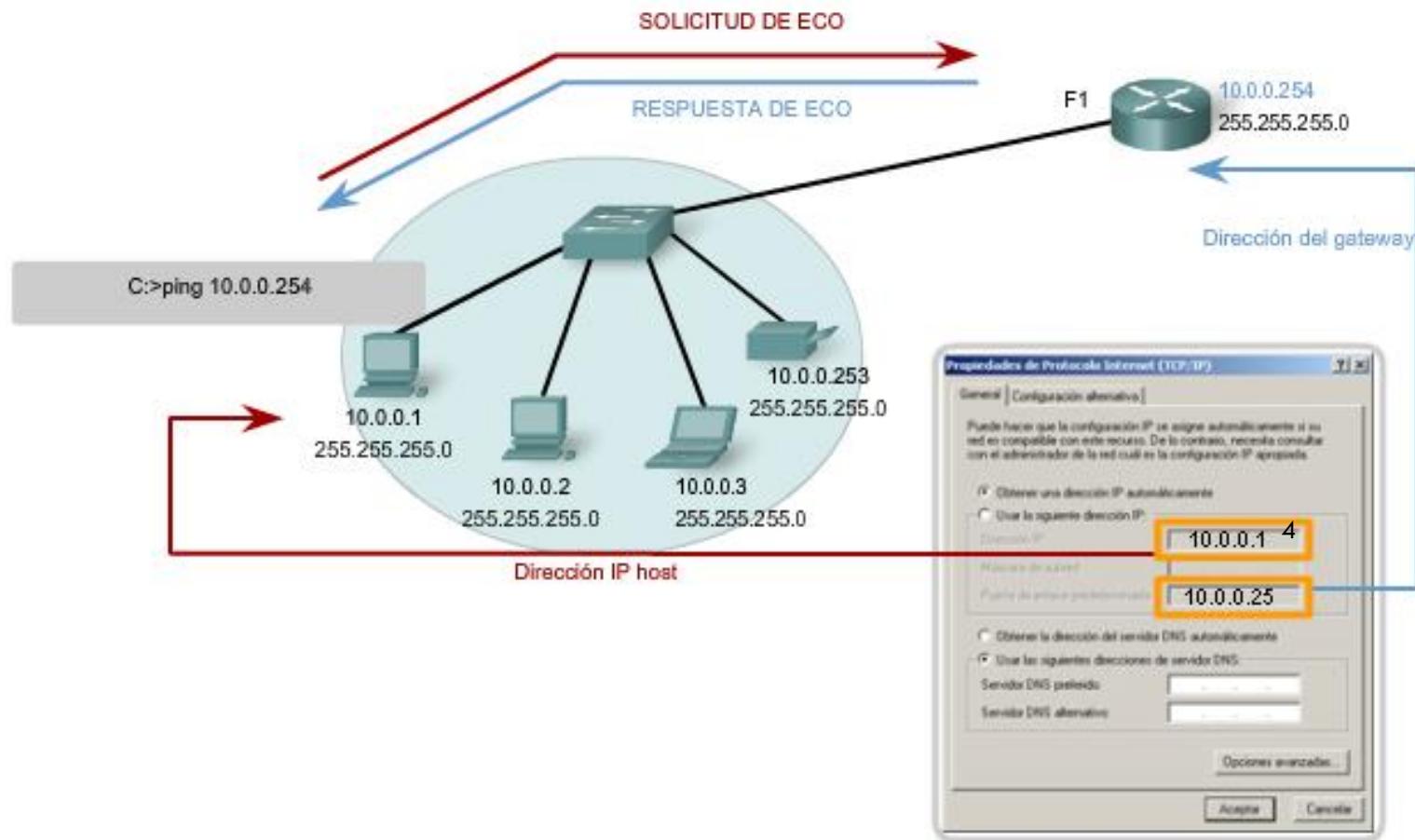
```
C:\Documents and Settings\acamposg>ping 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:

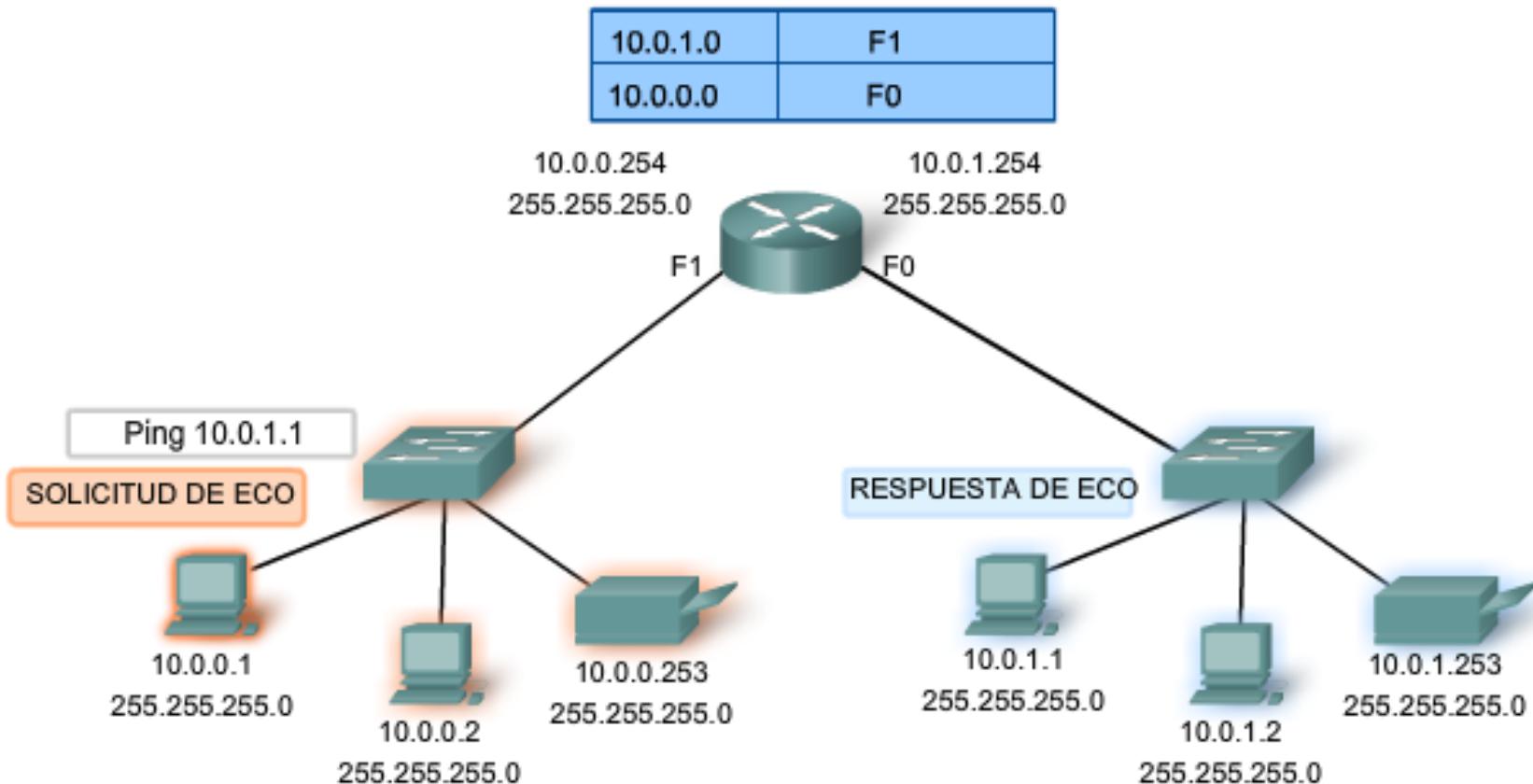
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

PING A LA PUERTA DE ENLACE



PING AL HOST REMOTO



TRACERT

Permite observar la ruta entre los host.

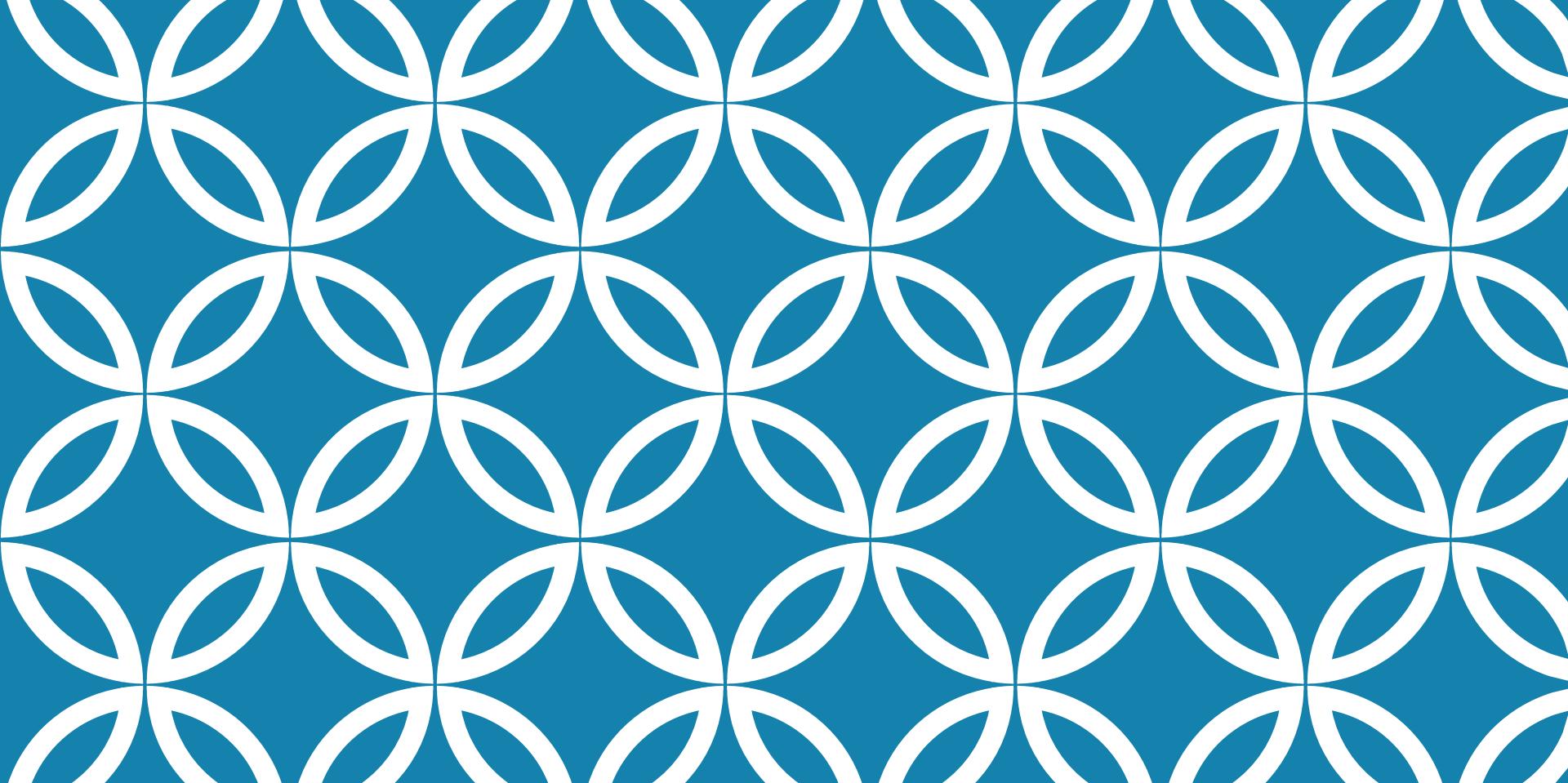
Genera una lista de saltos que se cumplieron satisfactoriamente a lo largo de la ruta.

```
C:\Documents and Settings\acamposg>tracert www.cisco.com
Traza a la dirección origin-www.cisco.com [198.133.219.25]
sobre un máximo de 30 saltos:

 1  32 ms   <1 ms   <1 ms  10.48.13.254
 2  1 ms    <1 ms   <1 ms  10.48.1.3
 3  5 ms    2 ms    3 ms   host-201-151-65-141.block.alestra.net.mx [201.151.65.141]
 4  16 ms   2 ms    2 ms   host-200-94-59-10.block.alestra.net.mx [200.94.59.10]
 5  4 ms    4 ms    5 ms   host-201-151-29-73.block.alestra.net.mx [201.151.29.73]
 6  3 ms    2 ms    2 ms   host-201-151-29-6.block.alestra.net.mx [201.151.29.6]
 7  31 ms   29 ms   31 ms  12.88.200.229
 8  71 ms   69 ms   70 ms  cr2.dlstx.ip.att.net [12.122.138.142]
 9  70 ms   69 ms   79 ms  cr2.la2ca.ip.att.net [12.122.28.178]
10  73 ms   69 ms   70 ms  cri.la2ca.ip.att.net [12.122.2.165]
11  70 ms   70 ms   69 ms  gar1.sj2ca.ip.att.net [12.123.30.331]
12  *       *       *      Tiempo de espera agotado para esta solicitud.
13  *       *       *      Tiempo de espera agotado para esta solicitud.
14  *       *       *      Tiempo de espera agotado para esta solicitud.
```

ICMP: INTERNET CONTROL MESSAGE PROTOCOL

- Suministra información sobre los problemas relacionados con el procesamiento de paquetes IP.
- Estos mensajes no son necesarios y a menudo no están permitidos por razones de seguridad.
- Proporciona mensajes de control y error y lo utilizan **ping** y **tracert**.
- Los mensajes ICMP que se pueden enviar son los siguientes:
 - Confirmación de host
 - Tiempo excedido
 - Redirección de ruta
 - Origen saturado
- Códigos de Destino inalcanzable:
 - 0 → red inalcanzable
 - 1 → host inalcanzable
 - 2 → protocolo inalcanzable
 - 3 → puerto inalcanzable



PLANIFICACIÓN Y CABLEADO DE REDES

LANS: LA CONEXIÓN FÍSICA

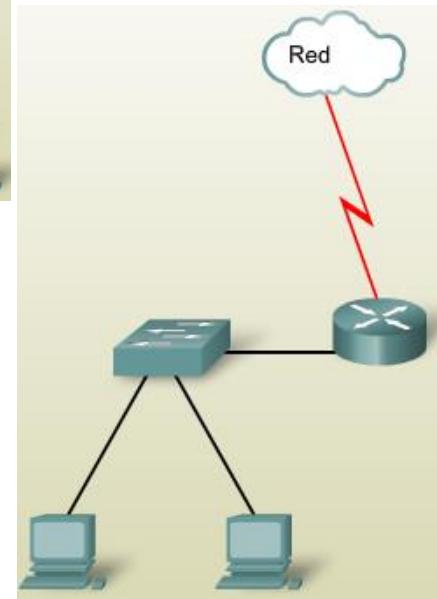
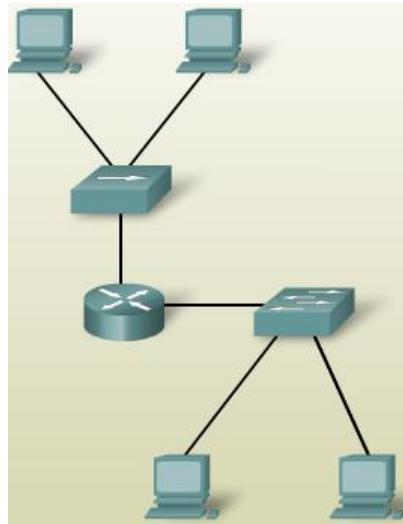
Principales dispositivos:

- Enrutador
 - Funciona como puerta de enlace para conectar la LAN a otras redes.
- Switch
- Hub
 - Ambos dispositivos conectan los dispositivos finales a la LAN.

DISPOSITIVOS DE INTERNETWORK

Enrutador

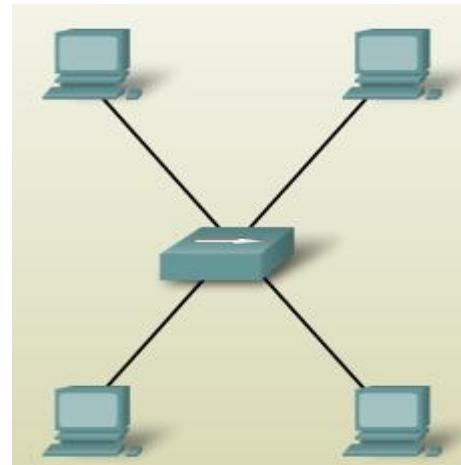
- Cada puerto del enrutador conecta con una red distinta
- Enruta los paquetes entre las redes
- Tiene la capacidad de dividir **dominios de difusión** y **dominios de colisión**.
- Interfaces LAN
 - Se conectan con UTP o fibra óptica.
- Interfaces WAN
 - Se conectan con cable serial dependiendo del modelo del enrutador.



DISPOSITIVOS DE INTRANETWORK

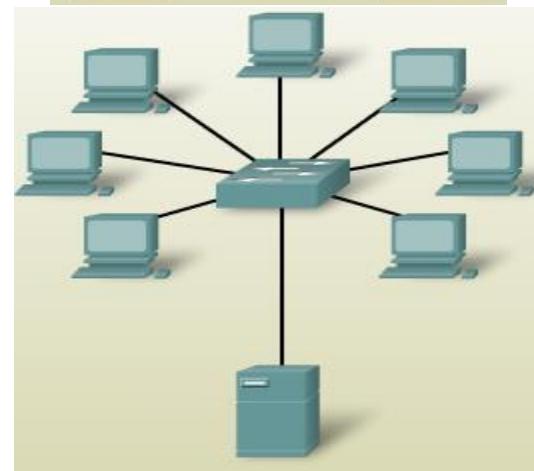
Hub

- Recibe la señal, la regenera y la envía por **todos** los puertos.
- LAN pequeña en donde los rendimientos son bajos y el presupuesto limitado.



Switch

- Recibe la señal, la regenera y la envía por el puerto destino.
- Segmenta dominios de colisión.
- Proporciona en cada uno de sus puertos un ancho de banda dedicado.



FACTORES PARA SELECCIONAR EL DISPOSITIVO

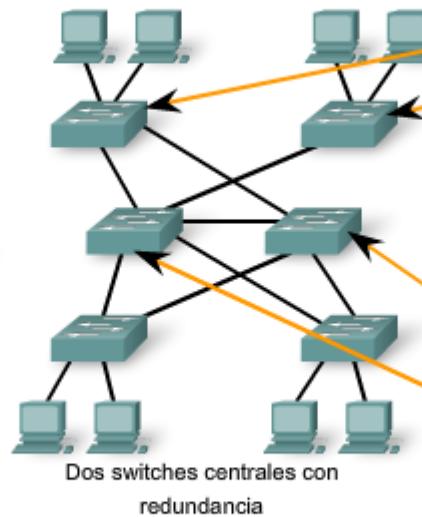
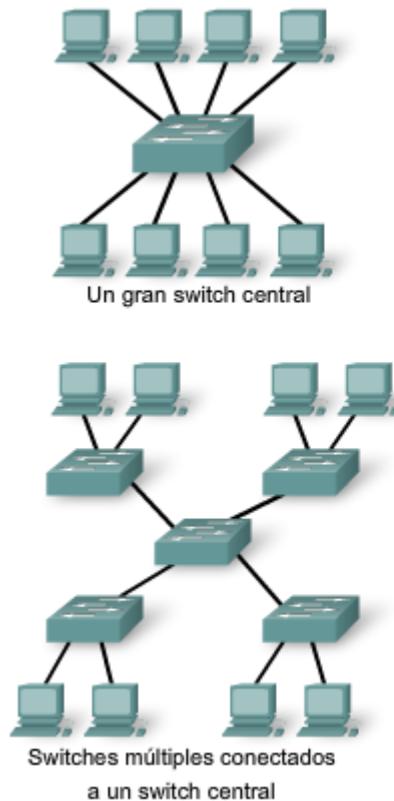


SELECCIÓN DE UN SWITCH

Factores a considerar

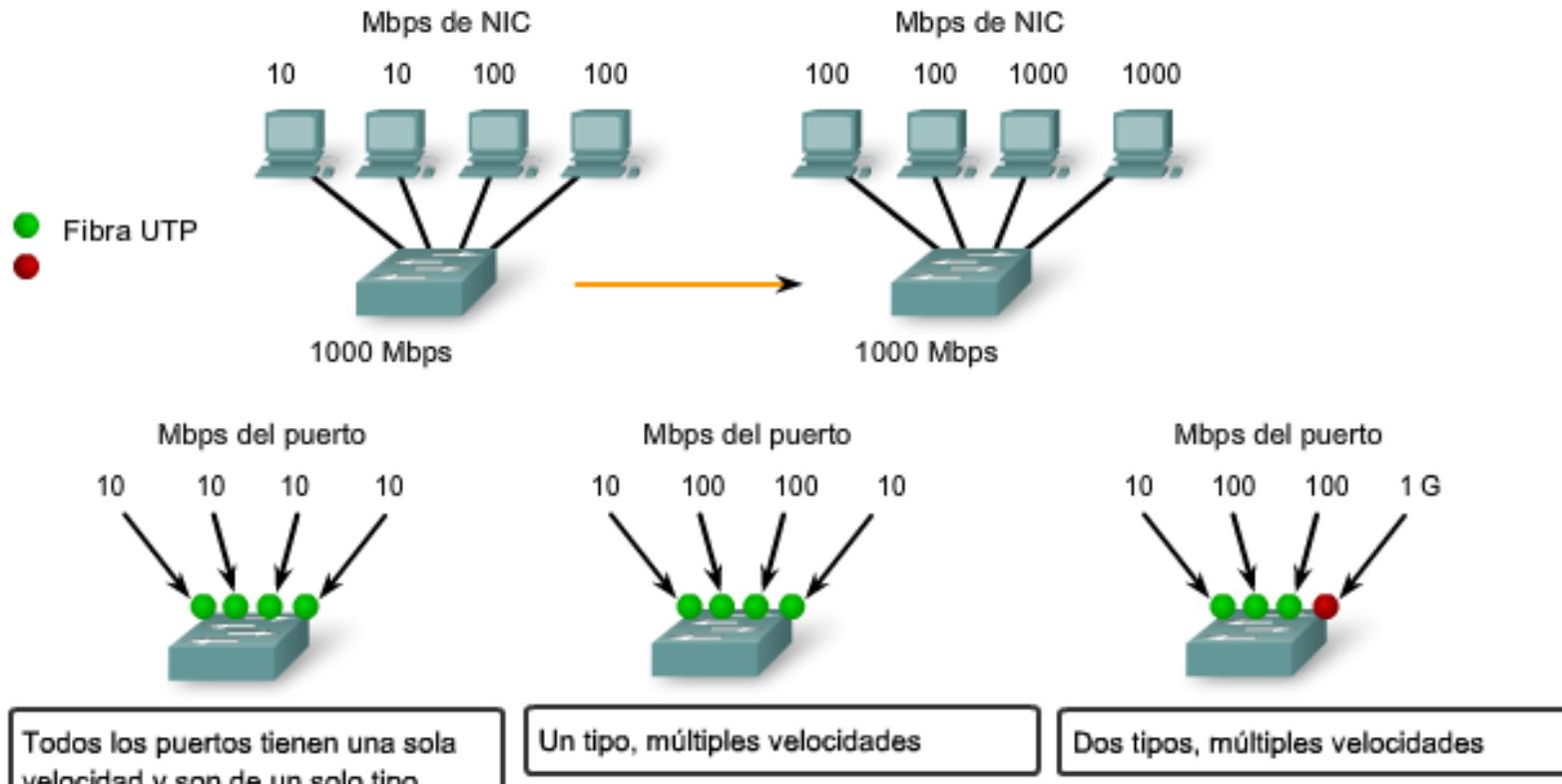
- Costo
 - Capacidad
 - Características de administración
 - Tecnologías de seguridad integradas
 - Tecnologías de conmutación
 - Redundancia

REDUNDANCIA



SELECCIÓN DE UN SWITCH

Velocidades, tipos y capacidad de expansión de los puertos



Algunos switches se pueden expandir con módulos adicionales para cumplir nuevos requisitos.

SELECCIÓN DE UN ENRUTADOR

Factores a considerar

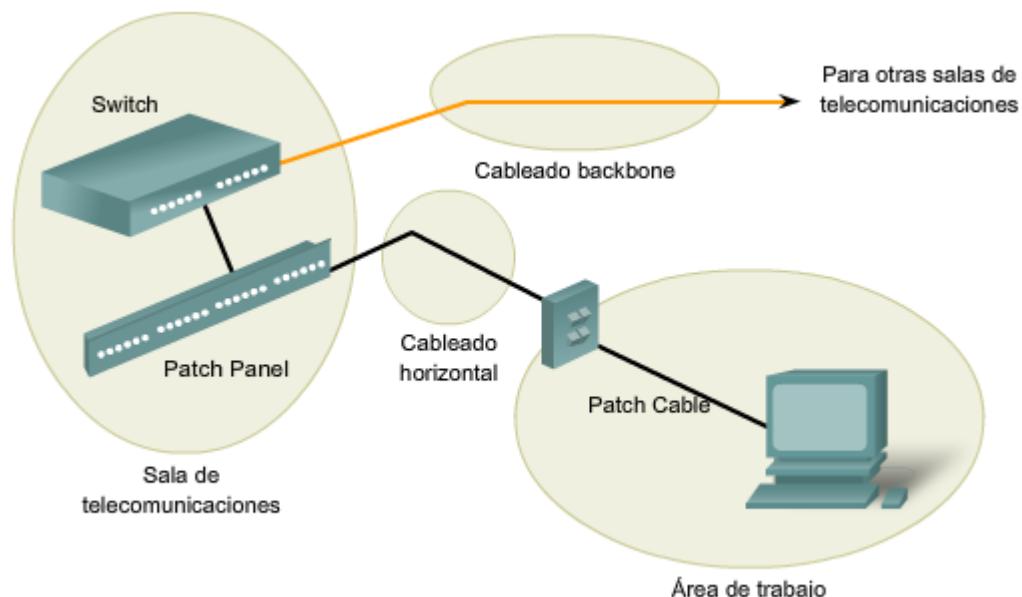
- Costo
- Velocidades de interfaces
- Expansibilidad en puertos e interfaces
- Medios
- Características del sistema operativo
 - Seguridad
 - Calidad y servicio (QoS)
 - Voz sobre IP (VoIP)
 - Enrutamiento con varios protocolos
 - Servicios especiales como NAT y DHCP.



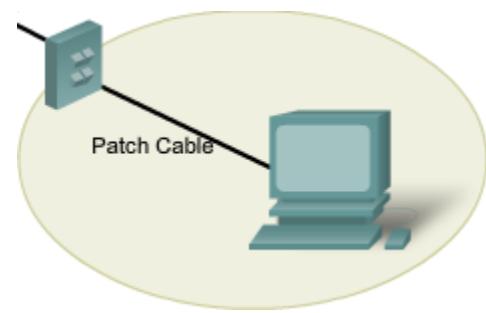
INTERCONEXIÓN DE DISPOSITIVOS

Instalación del cableado LAN, se debe tener en cuenta :

- Área de trabajo.
- Sala de telecomunicaciones conocida como instalación de distribución.
- Cableado horizontal conocido como cableado de distribución.
- Cableado *backbone* conocido como cableado vertical.



ÁREAS DE TRABAJO



Son las ubicaciones dedicadas a los dispositivos finales que los usuarios individuales utilizan.

Tienen un mínimo de dos *jacks* que se pueden usar para conectar a un dispositivo individual a la red.

Cable de conexión directa es el cable de uso más común en el área de trabajo.

- Conecta dispositivos finales, como computadoras, a una red.

Cuando se coloca un hub o switch en el área de trabajo, generalmente se utiliza un cable de conexión cruzada para conectar el dispositivo al jack de pared.

SALA DE TELECOMUNICACIONES

Es donde se realizan las conexiones a los dispositivos intermediarios.

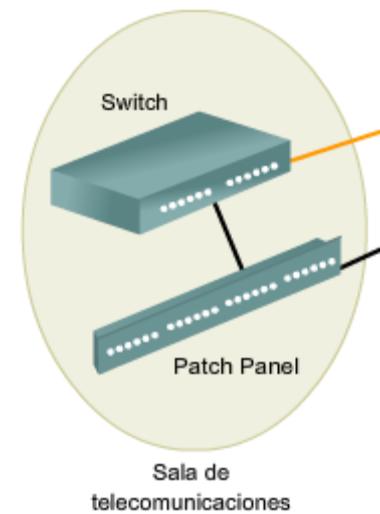
- Hub, switches, enrutadores y DSU, *data service units*.

Incluye los servidores utilizados por la red.

Patch cords sirven para realizar las conexiones

entre los patch panels.

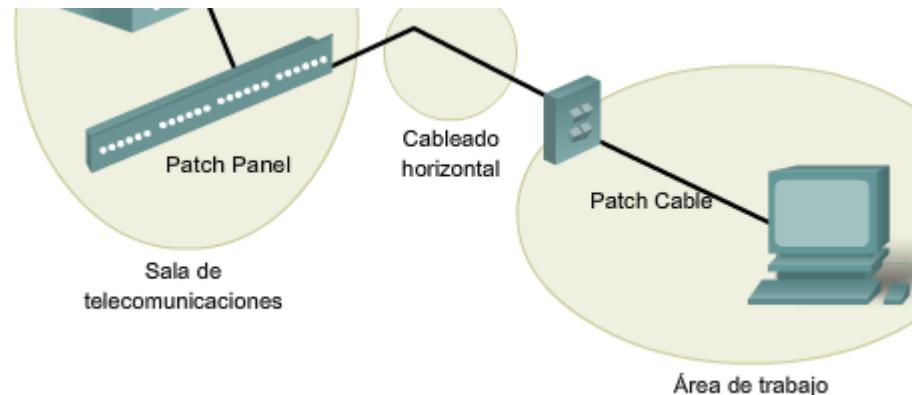
- Longitud de hasta 5 metros.



CABLEADO HORIZONTAL

Son los cables que conectan las salas de telecomunicaciones con las áreas de trabajo.

La longitud del cable no debe de exceder a los 90 metros, se conoce como **enlace permanente**.



CABLEADO BACKBONE O CABLEADO VERTICAL

Se refiere al cableado que se utiliza para conectar las salas de telecomunicaciones con las salas de los equipos.

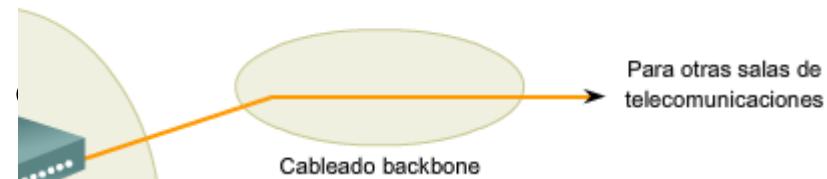
- Normalmente aquí se ubican los servidores.

Interconecta LAN entre edificios.

Se utiliza para el tráfico hacia y desde Internet.

Requiere de ancho de banda

- Fibra óptica.



TIPOS DE MEDIOS



Fibra



UTP



Inalámbrica

LONGITUD DEL CABLE

Longitud total =

- ✓ desde los dispositivos hasta el conector de pared.
- ✓ a través del edificio.
- ✓ cable desde el patch panel hasta el switch.
- ✓ cable entre edificios.

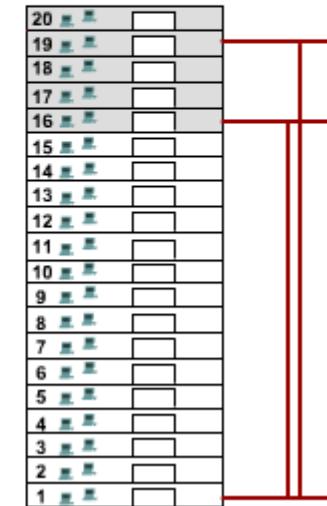
La distancia del cableado es un factor esencial en el rendimiento de la señal de datos. La atenuación de la señal y la exposición a una posible interferencia aumenta con la longitud del cable.



Las longitudes de los cables deben determinarse y coincidir con la tecnología utilizada.

Plano de piso

Edificio de varios pisos



Tipo de Ethernet	Ancho de banda	Tipo de cable	Distancia máxima
10Base-T	10 Mbps	UTP Cat3/Cat5	100 m
100Base-TX	100 Mbps	UTP Cat5	100 m
100Base-TX	200 Mbps	UTP Cat5	100 m
100Base-FX	100 Mbps	Fibra multimodo	400 m
100Base-FX	200 Mbps	Fibra multimodo	2 Km
1000Base-T	1 Gbps	UTP Cat5e	100 m
1000Base-TX	1 Gbps	UTP Cat6	100 m

Costo

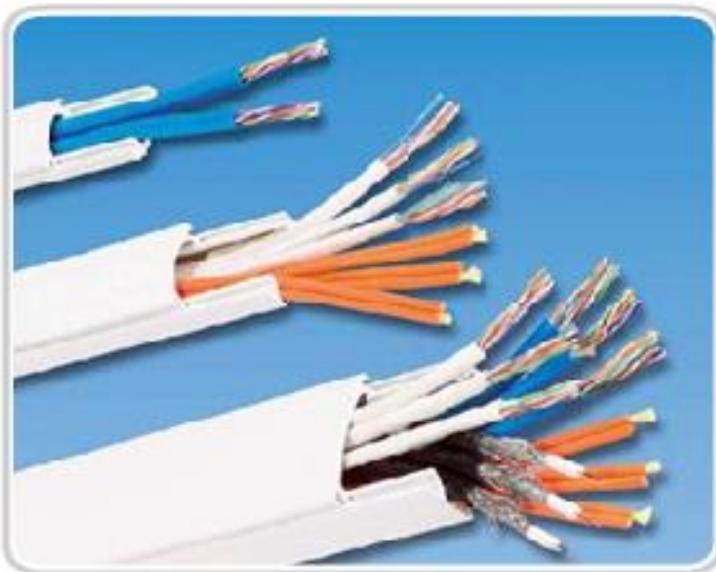
Deben de tener en cuenta las necesidades de rendimiento de los usuarios con el costo del equipo y cableado para conseguir la mejor relación costo/rendimiento.

Ancho de Banda

Servidor

- Mayor ancho de banda.
- Crecimiento a nuevas tecnologías.

FACILIDAD DE INSTALACIÓN



Canal para cable UTP



Canal para cable de fibra

INTERFERENCIA

Electromagnética (EMI)

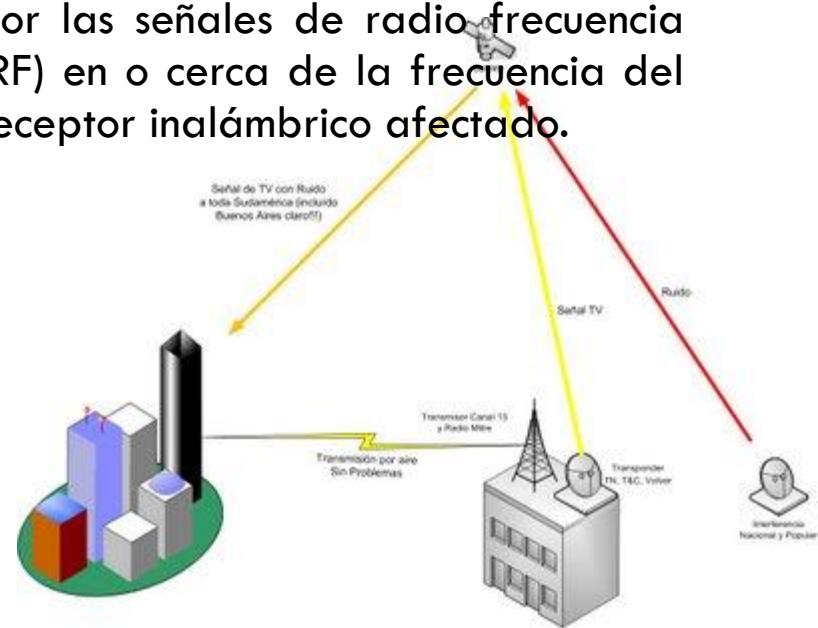
Se refiere a la interferencia en equipo de audio producida por dispositivos o cable "recogiendo" campos magnéticos en el ambiente.

Estos campos electromagnéticos pueden ser producidos por:

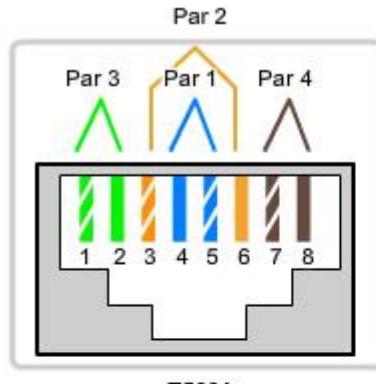
- luces fluorescentes,
- líneas de energía eléctrica,
- computadoras,
- televisores,
- monitores,
- transmisores de radio, y
- transmisores de televisión entre otros.

Por radiofrecuencia (RFI)

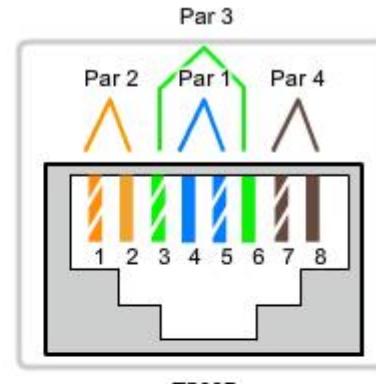
Este tipo de interferencia es causado por las señales de radio frecuencia (RF) en o cerca de la frecuencia del receptor inalámbrico afectado.



CONEXIONES LAN



T568A



T568B



T568A



T568B

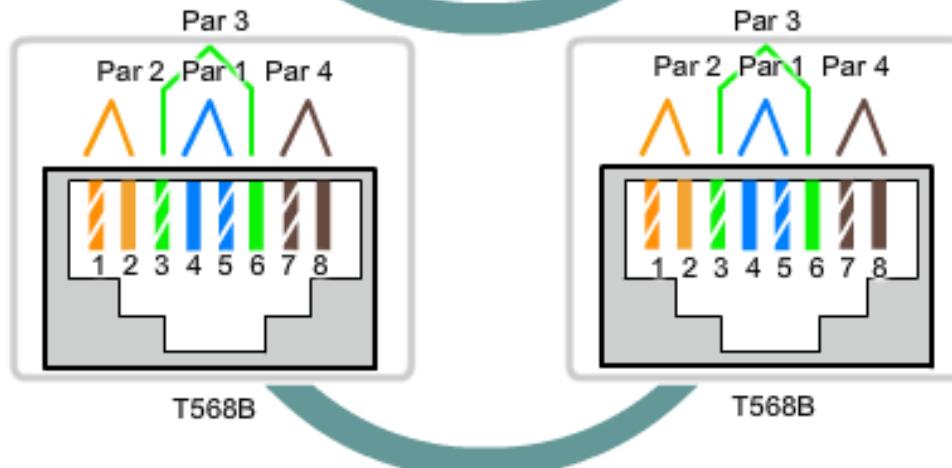
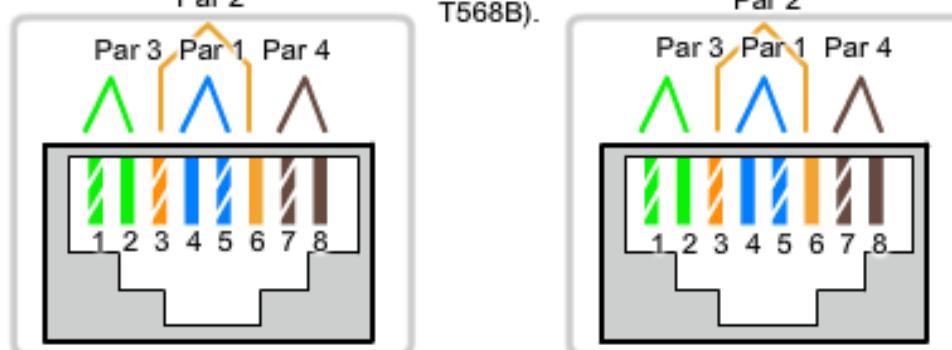
TIPO DE INTERFACES

MDI (interfaz dependiente del medio) utiliza un diagrama de pines normal de Ethernet. Pines 1 y 2 para transmitir, pines 3 y 6 para recibir.

MDIX (interfaz cruzada dependiente del medio). Los cables MDIX intercambian los pares transmisores internamente.

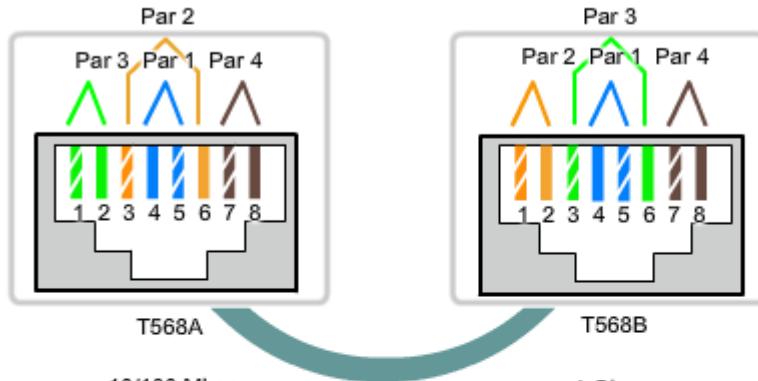
CABLE UTP DIRECTO

Los cables de conexión directa tienen la misma terminación en cada uno de los extremos (T568A o T568B).



CABLE UTP CRUZADO

Los cables de conexión cruzada tienen una terminación T568A en un extremo y una terminación T568B en el otro.



Los pins de transmisión en cada uno de los extremos se conectan a los pins de recepción del otro extremo.



CONEXIONES WAN

Conexiones seriales de 60 pines



RJ-11 de línea telefónica o
conexiones DSL

Router Cisco 827-4v



SERIALES: SMART SERIAL



Router: Serial inteligente macho



Red: Tipo de bloque Winchester macho

DCE Y DTE

DCE, Data Communications Equipment

- Dispositivo que suministra los servicios de sincronización con otro dispositivo.

DTE, Data Terminal Equipment

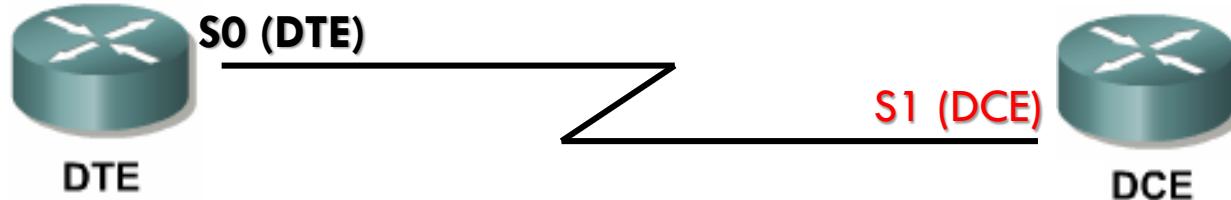
- Dispositivo que recibe los servicios de sincronización de otro dispositivo y realiza los ajustes necesarios.



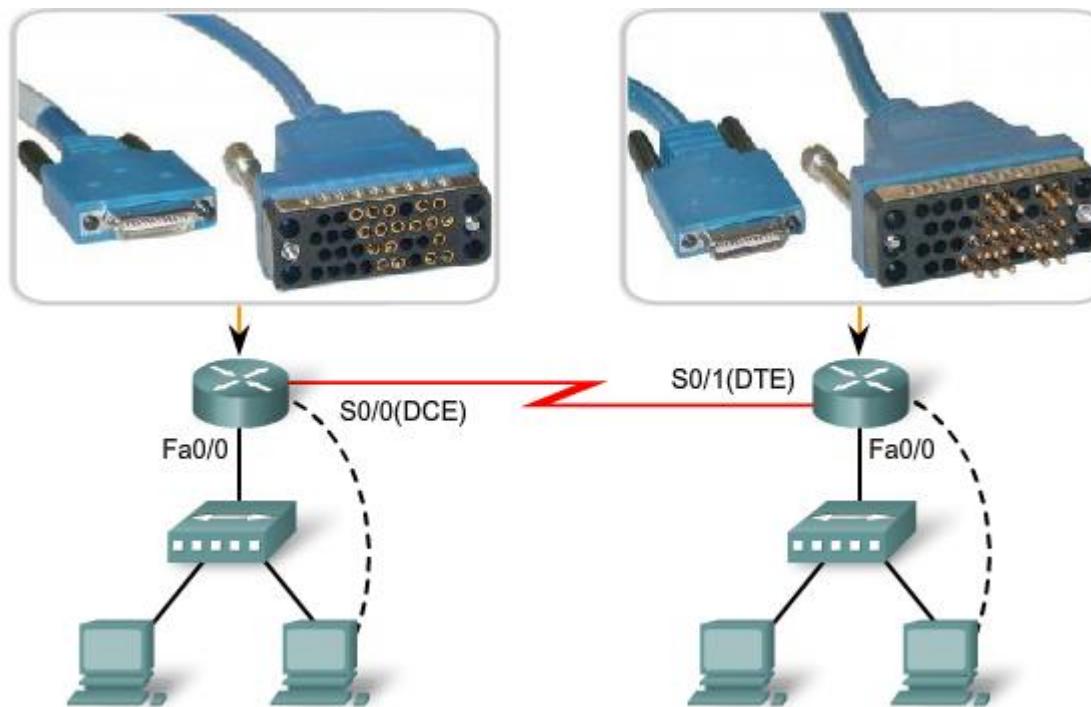
CONEXIÓN SERIE BACK-TO-BACK

En algunos de los casos el enrutador debe ser un DCE ya que se emplea en ambos extremos de la conexión.

En un entorno de prueba, uno de los enrutadores es un DTE y el otro un DCE **para proporcionar el reloj**.



CONEXIÓN WAN PUNTO A PUNTO



INTERCONEXIONES DE DISPOSITIVO

Interfaces o Puertos

▪ FastEthernet

- Conecta dispositivos LAN como computadoras, switches y enrutadores.

▪ Serie

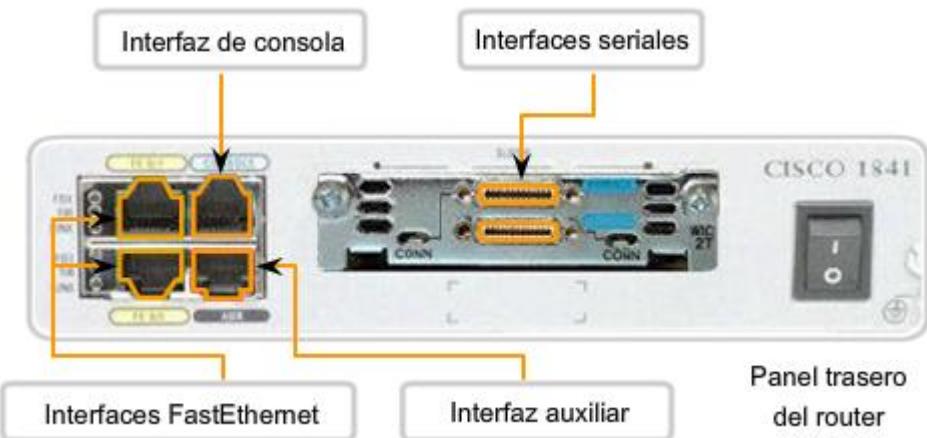
- Conecta dispositivos WAN a la CSU/DSU.

▪ Consola

- Se utiliza para configurar el enrutador o switch.

▪ Auxiliar

- Se utiliza para administrar el enrutador en forma remota. Normalmente un módem se conecta a esta interfaz.



Panel trasero
del router

PUERTO DE CONSOLA



Se necesita de este puerto para configurar el enrutador.

Para conectar el enrutador con la computadora se necesita un **cable rollover** con conectores RJ-45.

Rollover → cable de consola.

Se necesitará el adaptador USB-Serial, por lo que es necesario instalar el driver, el cual lo encontrarás en la página del **CNAP**.

- http://cnap.cem.itesm.mx/CNAP_ITESM_CEM/Material_CCNA.html

CONFIGURACIÓN DE EMULACIÓN DE TERMINAL

Pasos:

1.- Abrir la conexión

Inicio → Todos los programas → Accesorios → Comunicaciones → HyperTerminal



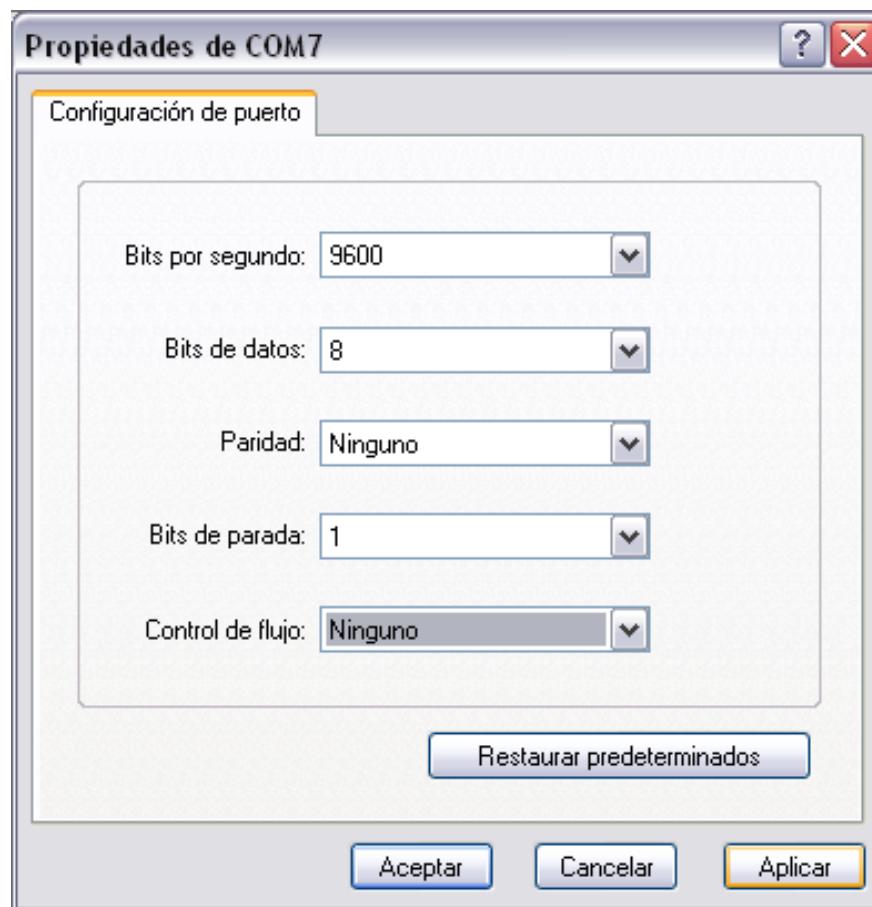
2.- Seleccionar el puerto

Si no estás seguro de que número de puerto es el driver que se instaló, verificalo en la siguiente ruta:

Inicio → Panel de Control → Sistema → Hardware → Administrador de dispositivos → Puertos (COM & LPT)



3.- Colocar las propiedades del puerto



CLI

Presione enter para acceder al CLI

```
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
```

Self decompressing the image :

```
#####|
```

Una vez que el dispositivo haya cargado conteste la pregunta con un **NO**

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
```

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no



CONFIGURACIÓN DE DISPOSITIVOS CISCO

El Cisco IOS provee a los dispositivos los siguientes servicios de red:

- Funciones básicas de enrutamiento y commutación.
- Acceso confiable y seguro a recursos en red.
- Escalabilidad de la red.

El IOS se almacena en la memoria *flash*.

El IOS se copia a la memoria RAM cuando el dispositivo arranca, lo que incrementa el rendimiento.

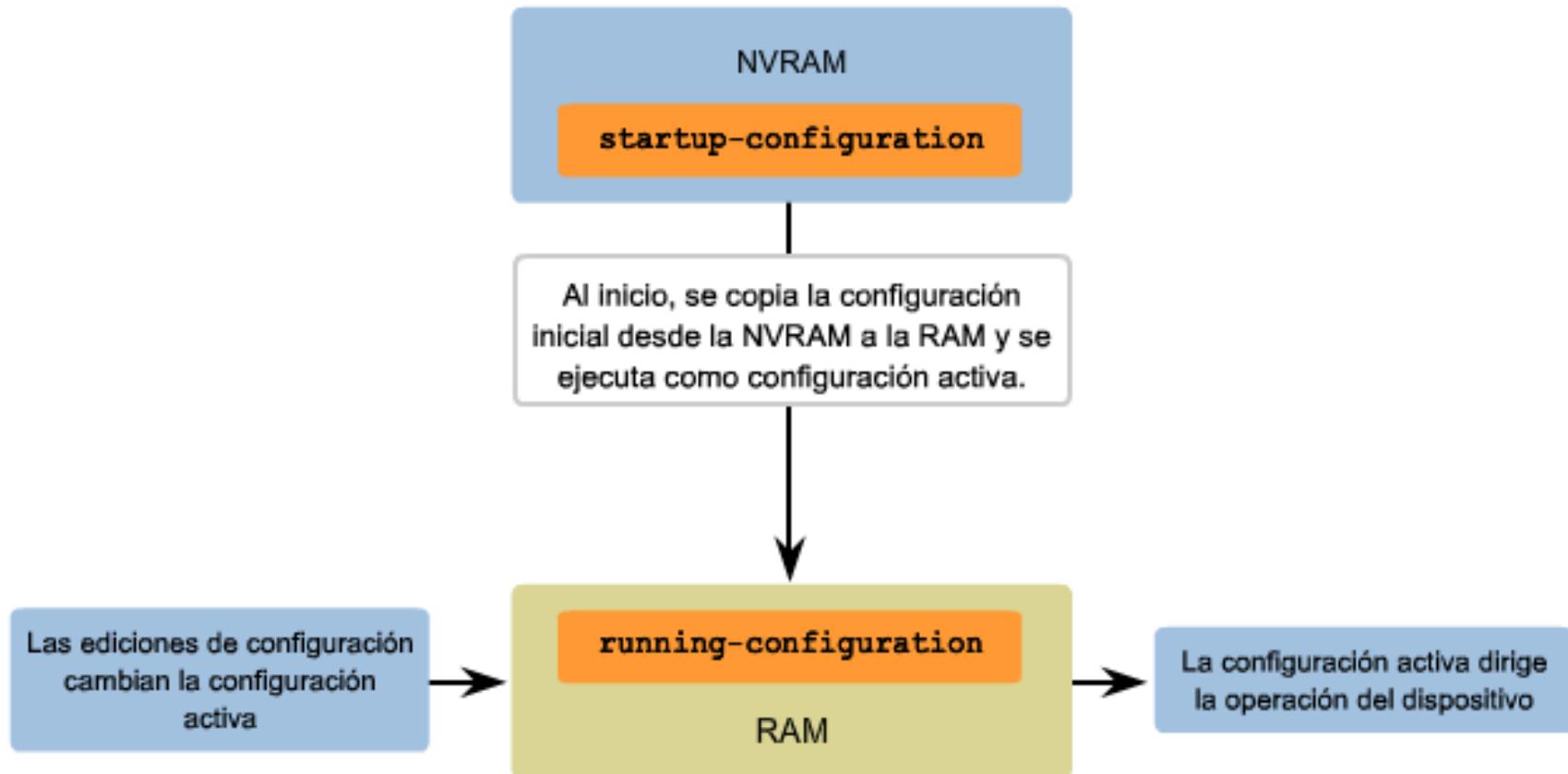
Se accede al IOS de un enrutador o switch a través de una Interfaz de Línea de Comandos (CLI).

MÉTODOS DE ACCESO AL CLI

Métodos más comunes son:

- **Consola**
 - usa una conexión serial de baja velocidad para conectar directamente un equipo al puerto de consola en el enrutador o switch.
 - **Uso**
 - Configuración de inicio del dispositivo de red.
 - Procedimientos de recuperación de desastres y resolución de problemas donde no es posible el acceso remoto.
 - Procedimientos de recuperación de contraseña.
- **Telnet o SSH**
 - Sirve para acceder en forma remota a la sesión CLI (Telnet).
 - SSH → método más seguro para acceso remoto (Secure Shell).
- **Puerto auxiliar**
 - Se establece la sesión con el CLI a través de una conexión telefónica.

ARCHIVOS DE CONFIGURACIÓN



MODOS DEL CISCO IOS

Modo	Descripción	Indicador
EXEC usuario	Muy limitado, permite los comandos ping y show version.	Router>
EXEC privilegiado	Examen detallado del enrutador. Depuración y verificación. Manipulación de archivos.	Router#
Configuración global	Configuración de parámetros globales o ingresar a otro submodos de configuración.	Router (config) #